PUBLIC
VERSION

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

In the Matter of the Application of SAN JOSE WATER COMPANY (U 168 W) for an Order authorizing it to increase rates charged for water service by $55,196,000 or 11.11% in 2025, by $22,041,000 or 3.99% in 2026, and by $25,809,000 or 4.49% in 2027	Application No. 24-01-001 Filed January 2, 2024

REBUTTAL OF SAN JOSE WATER COMPANY TO THE PUBLIC ADVOCATES OFFICE REPORT AND RECOMMENDATIONS ON PHYSICAL SECURITY RELATD CAPITAL IMPROVEMENT PROJECT AND EXPENSES

SAN JOSE WATER COMPANY
John Tang
Vice President of Regulatory Affairs
& Government Relations
110 West Taylor Street
San Jose, California 95110
Telephone: 408.279.7933
Facsimile: 408.279.7934
E-mail: john.tang@sjwater.com

Lori Anne Dolqueist
Nossaman LLP
50 California Street, 34th Floor
San Francisco, CA 94111-4707
Telephone: 415.438.7271
Facsimile: 415.398.2438
E-mail: ldolqueist@nossaman.com

May 31, 2024

SJWC Rebuttal Testimony Witnesses and Topics

Public Advocates Office Report and Recommendation	Public Advocates Office Witness	Topic(s) Covered
Expenses and Special Requests Chapter 8-9 Purchased Services	Timothy Gee	Purchased Services
On Expenses and Special Requests: Chapter 8-14 - Payroll	Timothy Gee	Additional Positions: Physical Security Specialist, Emergency Management Specialist, and Emergency Management Administrative Assistant
Expenses and Special Requests Chapter 20; Capital Improvement Projects 12-9	Kerrie Evans	Physical Security Improvement Capital Project

SJWC Rebuttal Testimony Attachments

Attachment A	Statement of Qualifications
Attachment B	Guard Service RFI Responses
Attachment C	Massachusetts Institute of Technology - Living Wage Study
Attachment D	American Society of Civil Engineers ASCE/EWRI 78-24
Attachment E	SJWC Index 5284 - Appendix C – AWWA G430-14 Standards Analysis
Attachment F	Physical Security CIP Process Flow Chart
Attachment G	Physical Security Presentation at Field Tour

REBUTTAL TESTIMONY OF MARK HATCHER
REGARDING
PHYSICAL SECURITY CAPITAL IMPREMENT PROJECT AND EXPENSES

Q1 Please state your name and business address.

A1 My name is Mark Hatcher. I work at 1221A S. Bascom Avenue, San Jose, CA 95128.

Q2 By whom are you employed, and in what capacity?

A2 I am employed by San Jose Water Company (SJW) and serve as the Manager of Physical Security.

Q3 Have you provided a description of your educational background and work experience?

A3 Yes, this description can be found in Attachment A.

Q4 What is the purpose of your testimony?

A4 The purpose of my testimony is to respond to the recommendation of the Public Advocates Office (Cal Advocates) that the Commission reject SJWC's request for additional expenses related to the Physical Security program, infrastructure, and site-specific mitigations. This rebuttal addresses the responses from the Cal Advocates regarding physical security improvements at San Jose Water Company (SJWC), as described below.

CHAPTER 8 OPERATIONS AND MAINTENANCE EXPENSE

Issue:

Cal Advocates recommends denying the increase in security guard service costs due to a lack of documentation but did not adequately review the documentation provided.

Cal Advocates further denies any additional staff, including necessary staff for Security and Emergency management mandated activities that otherwise would not be completed.

Cal Advocates Position: (Cal Advocates Testimony, in their Report and Recommendation on Expenses and Special Request on page 8-10 Purchased Services

Cal Advocates argues that the Commission should reject SJWC's request to reimburse the expense of paying security guards a living wage. Cal Advocates claims that this was undocumented, and no supporting documentation was provided. Cal Advocates did not deny the justification for the need for guard service.

SJWC submitted $1,618,470 in Purchased Services for security guard services to attract and maintain a quality guard service workforce without increasing headcount.

SJWC takes our regulatory obligations seriously, and as a result of recent studies, we have found perilous factors that demand action to reduce security risks if unabated.[1,2] The current conditions do not meet regulatory compliance expectations and expose ratepayers to the consequences of failures, including interruption or loss of water service. Ratepayers benefit from a protected water utility.[3]

The proposed physical security improvements at SJWC are necessary to meet regulatory standards and essential to addressing the unique challenges posed by urbanization, the unhoused population, and evolving security threats. By adopting a proactive and comprehensive approach, SJWC aims to ensure its water delivery systems' safety, reliability, and resilience. The rebuttal underscores the critical need for these improvements and the inadequacy of minimal, interim measures as suggested by the Cal Advocates.

We recognize that we cannot wholly remove risk or become invulnerable to threats to our water distribution systems.[4] SJWC describes the appropriate physical security size-fit throughout the 140-plus page Index 5284 Physical Security submission with the necessity to employ a combination of strategies that support protection from

[1] SJWC Index 5284 – Physical Security, page 41
[2] SJWC Index 5284 – Physical Security, page 51
[3] SJWC Index 5284 – Physical Security, page 40
[4] SJWC Index 5284 – Physical Security, page 10

intentional and unintentional acts, reduce the cost in response to those acts borne by ratepayers over time, and align our water system's security to industry standards. The current conditions described below were included in the original submission:[5]

- Physical security assets have outlived their useful life.
- The sophistication of bad actors has outgrown our defenses.
- Resiliency risk is due to the size and complexity of our systems, which have grown and evolved to support many more connected services over time, while physical security has not kept pace to support the criticality.
- Physical security measures no longer comply or align with current industry standards.
- The environment around us has changed, bringing ever-increasing urban challenges to more stations supporting more service connections at higher risks of operational stoppage.
- Changes in social construct since COVID-19 are leading to more mass casualty threats by firearm against SJWC employees.
- Reduced local law enforcement capacity to protect critical assets (including elevated law enforcement reluctance to engage in criminal enforcement of trespass and property crimes) has diminished utility security, resulting in SJWC having to be more self-reliant in hardening perimeters, greater visibility of critical operations through video management systems, cameras, and analytics, and access control with auditing.
- Process Control Systems networks (SCADA) reach further to the edge. An ever-increasing amount of technology in remote stations presents significant cybersecurity and operational vulnerabilities.

The rebuttal further highlights the critical aspects of SJWC's physical security measures, demonstrating compliance with regulatory requirements, emphasizing the necessity of the proposed improvements, and further allowing SJWC to continue to deliver safe and reliable water service.

[5] SJWC Index 5284 – Physical Security, page 41

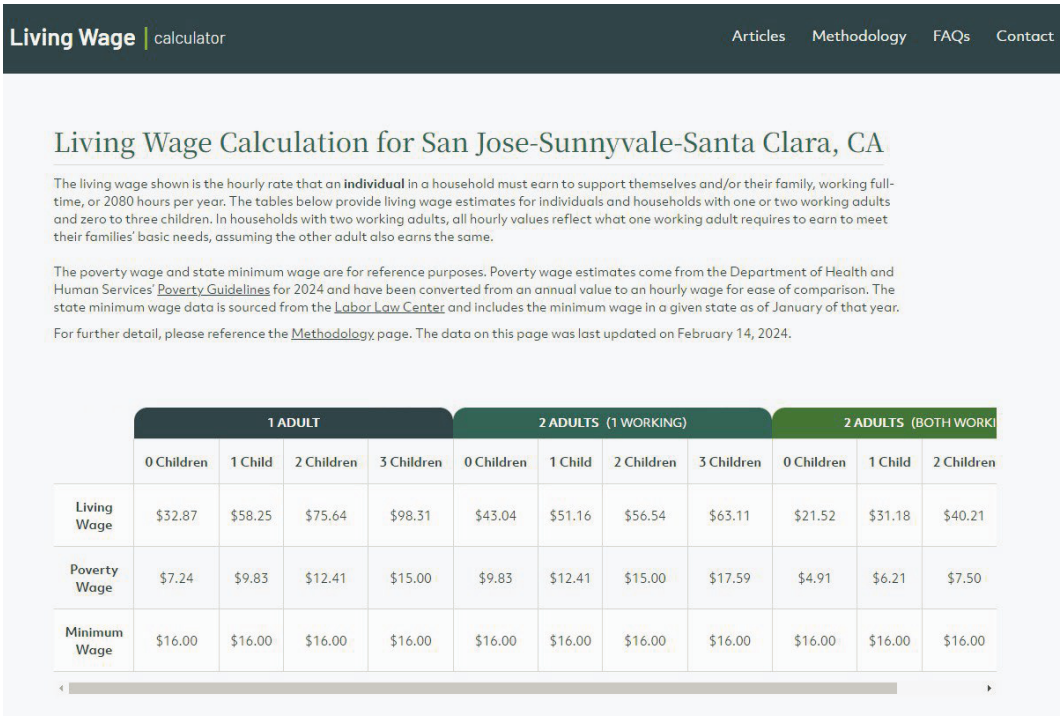
Guard Services Expense Rebuttal

Index 5284 addresses guard service costs in several ways.[6] SJWC provides the following clarifications.

1. Appendix D of the Index 5284 submission for Guard Service Cost Description states, "Current labor rates are ($21-an-hour) $6 an hour below San Jose living wage, resulting in difficulties hiring quality and reliable officers."
2. SJWC conducted a guard replacement cost study that included polling guard service companies to deliver a specific service model in Q1 2023[7] when the MIT living wage was $27-an-hour. Attachment B includes the responses to the guard service RFI cost polling. The represented service costs for the current guard utilization model are $1,443,468 and, $1,673,472, and $2,040,000 for an average cost of $1,718,980. The average bill rate is $67-an-hour per guard. This represents a $41.55-an-hour bill rate difference between the SJWC's bill rate in 2021 of $25.45 and the 2023 average study response rate of $67.
3. Index 5284 referenced guard pay rate and vendor margin as precipitous to problematic and poor historical performance. The submission further identified the need to engage in a living wage strategy as described in the Massachusetts Institute of Technology (MIT) analysis, a national standard for living wage study on a localized basis, including San Jose. [8] According to the MIT study, the current San Jose living wage is $32.87, $5 an hour higher than the originally referenced amount in the Index 5384 Physical Security submission.

Table of MIT Living Wage

[6] SJWC Index 5284 – Physical Security, page 61-63
[7] Attachment B – Guard Service RFI Poll Responses
[8] Attachment C – Massachusetts Institute of Technology (MIT) Living Wage Study



Living Wage | calculator

Articles Methodology FAQs Contact

Living Wage Calculation for San Jose-Sunnyvale-Santa Clara, CA

The living wage shown is the hourly rate that an **individual** in a household must earn to support themselves and/or their family, working full-time, or 2080 hours per year. The tables below provide living wage estimates for individuals and households with one or two working adults and zero to three children. In households with two working adults, all hourly values reflect what one working adult requires to earn to meet their families' basic needs, assuming the other adult also earns the same.

The poverty wage and state minimum wage are for reference purposes. Poverty wage estimates come from the Department of Health and Human Services' Poverty Guidelines for 2024 and have been converted from an annual value to an hourly wage for ease of comparison. The state minimum wage data is sourced from the Labor Law Center and includes the minimum wage in a given state as of January of that year.

For further detail, please reference the Methodology page. The data on this page was last updated on February 14, 2024.

	1 ADULT				2 ADULTS (1 WORKING)				2 ADULTS (BOTH WORKI		
	0 Children	1 Child	2 Children	3 Children	0 Children	1 Child	2 Children	3 Children	0 Children	1 Child	2 Children
Living Wage	$32.87	$58.25	$75.64	$98.31	$43.04	$51.16	$56.54	$63.11	$21.52	$31.18	$40.21
Poverty Wage	$7.24	$9.83	$12.41	$15.00	$9.83	$12.41	$15.00	$17.59	$4.91	$6.21	$7.50
Minimum Wage	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00

4. SJWC has over 195 water distribution stations to provide security, with 98% of those stations having no reliable intrusion detection, video visibility, or access control measures beyond padlocks that have been circulated for almost two decades.
5. AWWA G430-14, ASCE 56-10 (and the newer, May 2024, 78-24), and US EPA all require a safe separation of water distribution assets from unauthorized access.[9]
6. The escalation of service costs is unsustainable, and without proper electronic mitigation at SJWC water distribution stations, SJWC will not be able to reduce the dependency on guard service. As with many utilities, SJWC needs to convert guards from *patrol and report* where significant lost time and poor effort (as described in the regressive model[10]) to *respond and audit,* where technology is driving the automation of guard service for events and guard downtime, is consumed with audits and security posture validation. This change brings contractual performance opportunities for response times and audits completed with a reduced workforce for a lower ownership cost.

[9] SJWC Index 5284 – Physical Security, page 18
[10] SJWC Index 5284 Appendix E – Predictive Analysis Security Guard Patrol – Time Regression Model

7. Current workplace violence conditions necessitate quality security guard presence and vigilance.[11]

Cal Advocates Position: (Cal Advocates Testimony, in their Report and Recommendation on Expenses and Special Request on page 8-14, Labor and Payroll)

Physical Security Specialist

The request for physical security staffing from SJWC is unrelated to the Cupertino Lease. Instead, it resulted from realizing the extent of our security needs and the specific skills required to efficiently mitigate that risk across all of SJWC and requirements to meet mandated standards. SJWC physical security is a multifaceted approach, encompassing three key categories: program, infrastructure, and site specifics. Each category plays a vital role in our overall security strategy, ensuring we are well-prepared to handle potential threats.

The SJWC physical security Program can be described as the overall ecosystem where people, processes, and technology are applied across a definable set of responsibilities intended to lower risk while enhancing business optimization. The program is the fabric where workplace violence, policy and procedure, guard service, audits, planning and training, and investigations support SJWC security objectives.

The SJWC Physical Security Infrastructure creates, manages, and uses Video Management Systems (VMS), Physical Security Access Control Systems (PACS), Intrusion Detection Systems, computer networking, and computer systems to keep SJWC secure. This includes barriers like fencing and gates. Studies found that 98% of our water distribution systems (195 stations) don't have video of any kind, reliable PACS, or intrusion detection. Physical access control consists of a brass key-lock system that Cal Advocates agrees needs to be replaced with an updated smart lock system. SJWC uses thousands of the old locks. Programming requirements with dependencies that include the PACS architecture must be managed. Connectivity between PACS, VMS, and intrusion detection must be coordinated and maintained to make alerts actionable and coordinate guard service or law enforcement response.

[11] SJWC Index 5284 – Physical Security, page 37

SJWC physical Security Site Specifics encompass the application of the program and infrastructure in a specific environment where site conditions inside and outside of the facility must be integrated. Developing, maintaining, and applying the Master Station Design for Physical security will bring a definable approach with a predictable cost and measure of protection. From water distribution capital project planning security inclusions to design-build and commissioning. The delivered solution is scaled, planned for, and included in the station development.

Conclusion

SJWC requires diverse skills to support these efforts, but current staffing doesn't exist. Technology, project planning, where management and construction management, and physical security program accreditations Subject Matter Expert (SME) is needed. The FTE sought in the GRC intends to ensure those skills are ever-present. The lack of SMEs in physical security personnel can lead to future gaps that become more costly over time, delays in the implementation of security programs and construction, and less timely audits and investigations to identify root causes needed to prevent attacks on SJWC critical infrastructure.

Emergency Management Staffing

Given the rise in emergencies and disasters affecting water utilities, such as wildfires, earthquakes, and security breaches, along with increasing population density and regulatory demands, San Jose Water Company urgently needs an Emergency Management Specialist. This role is critical for assessing vulnerabilities, developing comprehensive response plans, and ensuring compliance with complex regulations. Additionally, with technological advancements and ongoing infrastructure upgrades, a specialist will enhance SJWC's preparedness and resilience, providing the community with continuous and safe water service. The specialist will also improve stakeholder coordination and increase community engagement, meeting Equity and Social Justice goals.

Argument for Hiring an Emergency Management Specialist at San Jose Water Company.

Though the Cal Advocates did not specifically deny the funding request for the Emergency Management Specialist, SJWC is reaffirming the necessity for the position.

Increased Emergencies and Disasters

The rise in the impact of wildland fires, earthquakes, physical attacks, sabotage attempts, and terrorist activities necessitates a robust emergency management posture. San Jose Water Company (SJWC) has faced significant challenges, including natural disasters, security breaches, and infrastructure emergencies, leading to multi-day downtimes affecting at-risk and underserved communities. These incidents highlight the need for a proactive approach to mitigate, prepare, respond, and recover from future crises. An Emergency Management Specialist can analyze past incidents, identify vulnerabilities, and implement security measures to minimize future risks, ensuring the resilience and continuity of water services.

Population Increase

The growing population density in the San Jose greater service area and the construction of multi-housing complexes directly impact emergency preparedness, response, and recovery efforts. Maintaining adequate water service for drinking and fire response is critical. An Emergency Management Specialist can assess vulnerabilities, develop comprehensive emergency response plans, and implement mitigation measures. The Emergency Management Specialist position ensures SJWC's capability to respond effectively to all incidents, safeguarding the community's water supply and enhancing overall emergency preparedness.

Emergency Risk and Resiliency Assessments

Regulatory requirements mandate periodic risk assessments to identify potential threats and vulnerabilities within the utility's environment. An Emergency Management Specialist can perform thorough evaluations and recommend necessary changes or improvements. This proactive approach ensures compliance with regulations and enhances the utility's ability to address potential risks, thereby safeguarding infrastructure and service continuity.

Regulatory Requirements

Compliance with complex regulations and standards for emergency management and preparedness is essential for water utilities. The intricate ecosystem of SJWC's water systems (one of the most sophisticated in the United States), coupled with the increasing frequency of incidents, necessitates dedicated expertise. An Emergency Management Specialist can manage ongoing

planning, preparedness, coordination, and community engagement activities, ensuring regulatory timeliness, quality, and scope. This specialist will:

- Planning and Preparedness: Develop and implement emergency response plans and conduct training exercises. These activities are time-consuming and require meticulous attention to detail. Additional personnel will improve the regulatory compliance and overall readiness of the community.
- Enhanced Coordination: Improve coordination with stakeholders, including government agencies, non-profits, and private sector partners, ensuring effective resource allocation during emergencies. This improved coordination directly benefits SJWC employees, customers, and stakeholders.
- Increased Community Engagement: Enhance community outreach efforts to improve overall preparedness and ensure compliance with Equity and Social Justice goals as outlined by the CPUC.

Technological Advancements

Advancements in technology, such as interoperability of communications, common operating platforms, and emergency mass notification systems, require specialized expertise. An Emergency Management Specialist can design and implement protocols, ensuring SJWC's readiness to respond and recover from incidents. This expertise provides the optimal functioning and readiness of technological systems critical for emergency management.

Infrastructure Expansion and Upgrades

SJWC's expansion and infrastructure upgrades present an opportunity to reassess and enhance emergency management infrastructure. Investments in emergency management must align with water distribution improvements in infrastructure capital. An Emergency Management Specialist can evaluate current capabilities, identify gaps, and propose improvements, ensuring that emergency management keeps pace with infrastructure development.

Emergency Management Administrative Assistant Staffing Rebuttal

The need for a Confidential Administrative Assistant (AA) for the Office of Emergency Management (OEM) and Security Department at San Jose Water Company (SJWC) is critical to

enhance the office's ability to respond to emergencies and disasters effectively. Currently, support for OEM & Security is a shared resource among 15 other supervisors, managers, directors, and Vice President, creating a significant administrative burden. A dedicated AA would manage the documentation unit during incidents, handle sensitive security investigation documentation, and oversee all documentation related to emergency management and security protocols, ensuring SJWC's readiness to respond and recover from incidents. Additionally, the AA would manage documentation for risk assessments, response plans, training, exercises, and after-action reports.

Argument for Hiring a Confidential Administrative Assistant at San Jose Water Company

Though the Cal Advocates did not specifically deny the funding request for the Confidential Administrative Assistant, SJWC is reaffirming the necessity for the position.

Key factors affecting the workload and the need for dedicated support include

Increased Emergencies and Disasters: SJWC has faced various incidents, including natural disasters, infrastructure emergencies, security breaches, and threats of violence, leading to multi-day downtimes and significant risks to at-risk communities. Strengthening the emergency management posture is essential.

Population Increase

The growing population density and ongoing construction of multi-housing complexes in San Jose increase the demand for emergency preparedness, response, and recovery to maintain proper water service for drinking and fire response.

Emergency Risk and Resiliency Assessments

Regulatory requirements mandate periodic risk assessments to identify potential threats and vulnerabilities. A dedicated AA would help manage the extensive documentation required for these assessments.

Regulatory Requirements

Compliance with emergency management and preparedness standards is essential. The AA would support planning, preparedness activities, enhanced coordination with stakeholders, and increased community engagement, ensuring regulatory timeliness and improving overall community readiness.

- Planning and Preparedness: Developing emergency response plans and conducting training exercises are administratively intensive tasks that require meticulous attention. The AA would enhance the quality and scope of these activities.
- Enhanced Coordination: During emergencies, the AA would help improve coordination with government agencies, non-profits, and private sector partners, ensuring effective resource allocation.
- Increased Community Engagement: The AA would support community outreach efforts, improving preparedness and meeting Equity and Social Justice goals as outlined by the CPUC.

Technological Advancements

Managing advancements in technology, such as communications interoperability and emergency mass notification systems, requires specialized expertise. The AA would ensure these systems are ready for emergencies.

Infrastructure Expansion and Upgrades

SJWC's ongoing infrastructure upgrades present an opportunity to enhance emergency management infrastructure. The AA would evaluate and propose improvements to align with these expansions.

Confidentiality

SJWC requires an administrative assistant to handle confidential information, including termination preparations, workplace violence investigations, and HR-protected information. This classification is not compatible with the existing staffing where confidential matter can not be shared.

CHAPTER 20 SAFETY, SECURITY & EMERGENCY MANAGEMENT

Issue:

Cal Advocates recommends the Commission approve a limited budget based on a five-year spending history and maintain existing surveillance equipment in the amount of $906,123 while denying SJWC's requests for $5,054,900 for 2024, 5,275,300 for 2025, and 5,517,800 for 2026. Cal Advocates Position: (Cal Advocates Testimony, Report and Recommendations on Capital Improvement Projects, page 12-9)

Cal Advocates in their Report and Recommendation on Capital Improvement Project for Physical Security Improvement on page 12-9

The dissensus between Cal Advocates and SJWC involves calculating capital improvement costs for security enhancements.[12] The Cal Advocates did not disagree with the need for physical security improvements. They prefer fixed bid proposals for replacing ineffective security measures with similar ones.[13] However, SJWC finds this approach oversimplistic due to the rapidly evolving nature of security challenges. These include changes in urbanization, the inevitable challenges brought by the ever-increasing number of unhoused individuals, evolving criminal methods, cybersecurity regulations at the edge of our operational networks (including station SCADA and MCCs), and reduced local law enforcement capacity and willingness to respond to service calls. Considerable water distribution utilization site changes have occurred since we installed the security measures many years ago, and the approach to evaluating, designing, and building mitigation has become more complex as a result.

To properly size-fit physical security at SJWC, we must recognize that the changing security complexities described above have evolved in one of the country's most complex water distribution systems. Station utilization has also changed over time, while physical security has not. SJWC must use a more responsible workflow than what Cal Advocates describes. We must not look backward to arrive at a budget but rather at the risks, asset types, reliance on those assets, and likelihood of derogatory occurrences. Site risk and hazard assessments must be completed

[12] Public Advocates Office Report and Recommendations – Public Version, page 8-9 and 8-10
[13] Public Advocates Office Report and Recommendations – Confidential Version, page 16-5

and used to develop site-specific mitigation plans that ensure design/build projects capture the necessary internal and external considerations.

SJWC is acutely aware of our regulatory obligations, and recent security studies have revealed perilous factors that necessitate immediate action to mitigate security risks. These conditions fall short of regulatory compliance standards and expose ratepayers to the potential consequences of failures, such as water service interruptions, water contamination, or loss of customer confidence, which could lead to civil unrest. The protection of our customers is paramount.[14]

The proposed physical security improvements at SJWC are necessary to meet regulatory standards and are essential for addressing the unique challenges posed by urbanization and evolving security threats. SJWC experienced a death of an intruder when he attempted to steal copper and became electrocuted. In another recent case, an arsonist lit fire to a PLC at a water tank serving our ESJ community resulting in a strategic well field being taken offline for days. Index 5284 Physical Security[15] provides additional instances of vandalism, theft, and sabotage.

By adopting a proactive and comprehensive approach, SJWC aims to ensure its water delivery systems' safety, reliability, and resilience. The rebuttal underscores the critical need for these improvements and the inadequacy of minimal, interim measures as suggested by the Cal Advocates.

SJWC recognizes that we cannot wholly decouple from risk or become invulnerable to threats to our water distribution systems.[16] SJWC describes the appropriate physical security size-fit throughout the 140-plus page Index 5284 Physical Security submission with the necessity to employ a combination of strategies that support protection from intentional and unintentional acts, reduce the cost to ratepayers over time, and the need for proper alignment to industry standards. The current conditions described below were included in the original submission:[17]

- Physical security assets have outlived their useful life.
- The sophistication of bad actors has outgrown our defenses.

[14] SJWC Index 5284 – Physical Security, page 40
[15] SJWC Index 5284 – Physical Security, pages 58-62
[16] SJWC Index 5284 – Physical Security, page 10
[17] SJWC Index 5284 – Physical Security, page 41

- Resiliency risk is due to the size and complexity of our systems, which have grown and evolved to support many more connected services over time, while physical security has not kept pace to support the criticality.
- Physical security measures no longer comply or align with current industry standards.
- The environment around us has changed, bringing ever-increasing urban challenges to more stations supporting more service connections at higher risks of operational stoppage.
- Changes in social construct since COVID-19 are leading to more mass casualty threats by firearm against SJWC employees.
- Reduced local law enforcement capacity to protect critical assets (including elevated law enforcement reluctance to engage in criminal enforcement of trespass and property crimes) has diminished utility security, resulting in SJWC having to be more self-reliant in hardening perimeters, greater visibility of critical operations through video management systems, cameras, and analytics, and access control with auditing.
- Process Control Systems networks (SCADA) reach further to the edge. An ever-increasing amount of technology in remote stations presents significant cybersecurity and operational vulnerabilities.

The Cal Advocates' historical spending approach is problematic because it underestimates the requirements to resolve the security problem. By engaging in past practices of under-investing in physical security, Cal Advocates fails to resolve the physical security debt that has been compounding over many years. The past practice of the Cal Advocates' reluctance to invest in physical security, once considered suboptimal, has now reached a negligence threshold requiring action.

SJWC has over 250 water distribution stations that require security, with over 98% of those stations having no reliable intrusion detection, video visibility, or access control measures beyond padlocks that have been in circulation for almost two decades. Cal Advocates argues for the maintenance of existing systems only. Fencing and gates, many installed many decades ago, were found to require replacement after living beyond their useful life, can be climbed over, cut with simple hand tools, and do not comply with current industry and regulatory standards. Studies have also found that the utilization of stations has changed over the years while the security has

not, resulting in vulnerabilities becoming more and more problematic to the health and reliability of our system.

Lastly, SJWC stations with the highest crime rates are located in ESJ communities where water is locally sourced and delivered, requiring an elevated level of security.

SJWC recommends that the Commission approve the budget as originally proposed.

Review of SJWC's Physical Security Capital Projects

SJWC enjoys the opportunity to present a detailed evaluation of the cost calculations for these projects and the rationale behind the necessity of these mitigations based on the information from the Index 5284 documents submitted to the California Public Utilities Commission (CPUC).

Cost Calculations for Physical Security Capital Projects

1. **Comprehensive Assessment Approach**: SJWC employed a detailed and systematic approach to assess the costs associated with physical security improvements. This involved:
    a. Conducted thorough site assessments and identified vulnerabilities at critical infrastructure locations.
    b. Engaging a nationally recognized consultant, Setracon, a risk assessment consultant, to perform independent threat and vulnerability assessments and provide expert recommendations.
2. **Breakdown of Costs**: The cost calculations included several key components, such as:
    a. Physical Barriers: Installation of fences, gates, and barriers to control access and protect perimeter areas.
    b. Advanced Security Technologies: Deployment of CCTV systems, intrusion detection systems, and access control systems to enhance real-time monitoring and response capabilities.
    c. Personnel Costs: Expenses related to hiring security personnel and providing necessary training and equipment.
3. **Justification for Costs**: SJWC's cost justification was based on industry standards, regulatory requirements, and best practices for physical security in the water utility sector. The costs reflect the necessary investments to mitigate

identified risks and ensure alignment with AWWA G430-14, American Society of Civil Engineers ASCE/EWRI 78-24,[18] and AWIA requirements. [19,20]

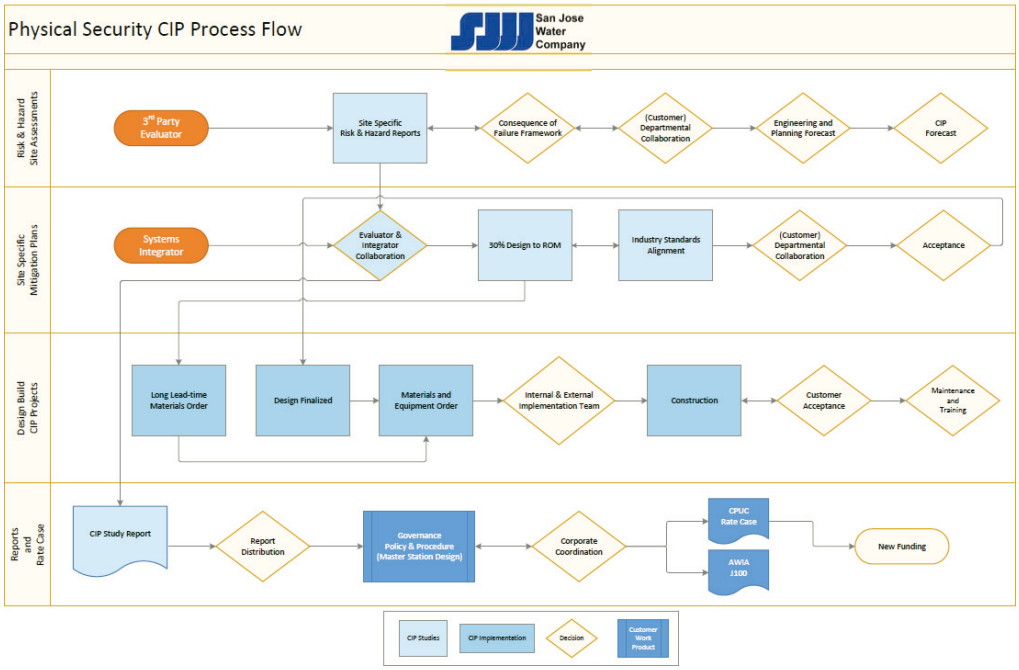
4. **Cost Estimates**: SJWC worked with Setracon, SLOAN Security Group, a nationally recognized physical barrier contractor, SLOAN Security Group, and Convergint, a leader in utility electronic mitigation, to develop a cost estimate by water distribution asset type. These fundamentals, in conjunction with site-specific environmental details, were used to calculate the unique feature requirements of each described site and provide pricing.
5. **Security Divergence**: Some site locations only have physical security upgrades associated with them while others have water distribution capital projects requiring physical security influence. SJWC requires internal and external engineering collaboration to reduce costs and apply the appropriate physical security apparatus to the intended site utilization in the future.

Development Process

Physical security in a complex water distribution system with aged security infrastructure cannot be approached in a simple estimate to rip-and-replace. A cost-basis, collaborative, and inclusive methodology is required to garner the intended result at the lowest cost. Attachment F describes the process of taking risk and hazard reporting and incorporating it into site mitigation plans for design/build. The flow chart encompasses the participation of vendors and internal stakeholders and ensures a cohesive approach with predictable and definable achievements.

Physical Security CIP Process Flow Chart[21]

[18] Attachment D - American Society of Civil Engineers ASCE/EWRI 78-24
[19] SJWC Index 5284 – Physical Security, page 18
[20] SJWC Index 5284 - Appendix C – AWWA G430-14 Standards Analysis – Rebuttal Attachment E
[21] Attachment F



Since the submission of Index 5284 Physical Security, SJWC has begun to develop Master Station Designs for Physical Security. These plans classify physical security requirements for water distribution assets by type and expand them over time as specific projects offer both details and differences in approaches to problem-solving. This endeavor reduces engineering costs significantly, cuts time estimates, and allows for future planning based on an accepted standard and methodology. The Master Station Design supports the inclusion of regulatory standards in the design to ensure consistent compliance with proximal mitigation of recognized and documented risks. The Master Station Designs for Physical Security also support a predictive approach for vendors, internal operations, and facilities support. SJWC provided the outcomes of these detailed anticipated expenditures as part of the data request process, KKE-004.

SJWC RATIONALE FOR PHYSICAL SECURITY MITIGATIONS

Urbanization and Increased Threats

The urban environment around SJWC's infrastructure has significantly increased the risk of unauthorized access and potential sabotage. High population density and the proximity of residential and commercial buildings necessitate robust physical security measures to protect water

supply systems. Urban problems like unhoused[22] people encroaching on SJWC stations bring an unpredictability of threat to water distribution system performance, including failures. The volume, variety, and velocity of mentally ill-related attacks completely change the paradigm of threat characterization (saboteur), where low-frequency yet high-risk situations map against a low threat likelihood.[23] Mentally ill who attack SJWC water distribution assets significantly change the frequency of probability due to the ever-increasing numbers at our gates and fence lines. The unhoused face stressors, unlike other people. Hunger, safety, inclement weather, health and sickness, mobility, and societal deaminization all play a part. Stress, combined with drug and alcohol abuse with no support system, often results in varying degrees of unabated mental illness. This manifestation blurs the lines of vandal, criminal, and saboteur found in many security standards because the definable motivation of each of those characteristics becomes irrelevant if the outcome of an attack is the same and the propensity for an attack is elevated due to the volume, variety, and velocity in the number of destructive events.

Aging Infrastructure

Many of SJWC's current security systems, such as gates and padlocks, are outdated and no longer sufficient to deter modern threats. They have also succumbed to fallen trees and trespassers cutting fence fabric with hand tools. Upgrading these systems is critical to maintaining the integrity and safety of water delivery infrastructure.

Compliance with Regulatory Standards

The proposed security improvements are in line with the requirements set forth by the AWWA[24], ASCE/EWRI[25], and AWIA. These standards mandate comprehensive risk assessments, physical barriers, and advanced security technologies to protect critical infrastructure.

Advanced Security Technologies

[22] SJWC Index 5284 – Physical Security, page 34
[23] Wallace. (2024). *Empirical Risk Analysis Methodology for Adversarial Threats against Critical Infrastructure*. Journal of Infrastructure Systems, volume 30, Issue 1
[24] Attachment E – American Water Works Association (AWWA) G430-10
[25] Attachment D - American Society of Civil Engineers (ASCE) & Environmental & Water Resources Institute (EWRI) 78-24

Deploying advanced security technologies like CCTV, intrusion detection systems, and smart locks provides multiple layers of security and brings efficiency opportunities to the system as a whole. These technologies allow for real-time threat detection, incident documentation, and rapid response, which are crucial for mitigating risks and ensuring the safety of water supplies. The escalation of guard service costs is unsustainable, and without proper electronic mitigation at SJWC water distribution stations, SJWC will not be able to reduce the dependency on guard service. As with many utilities, SJWC needs to convert guards from patrol and report where significant lost time and poor effort (as described in the regressive model) to respond and audit, where technology is driving the automation of guard service for events and guard downtime, is consumed with audits and security posture validation. This change brings contractual performance opportunities for response times and audits completed with a reduced workforce for a lower ownership cost.

Impact Analysis and Risk Mitigation

SJWC has conducted detailed impact analyses to understand the potential consequences of security incidents, including financial losses, public health risks, and service disruptions. The proposed mitigations are designed to address these risks effectively and ensure resilience against a wide range of threats.

Mitigation Strategies and Cost-Effectiveness

The Cal Advocate's recommendation to adopt interim repairs and retrofits overlooks the long-term benefits and cost-effectiveness of comprehensive security upgrades. SJWC's proposed improvements are based on a holistic, proactive approach that incorporates advanced technologies and robust security measures to ensure sustained protection against evolving threats while improving business optimization.

Impact Analysis and Risk Calculation

SJWC has developed detailed impact analyses and risk calculations for critical infrastructure locations. These analyses quantify the potential consequences of security incidents, including disruptions to water supply, financial losses, and harm to public health. Such rigorous assessment ensures that resources are allocated effectively to mitigate the highest risks.

Workplace Violence

Current workplace violence conditions necessitate quality physical security apparatus and vigilance.

In the realm of physical security, entropy, a concept borrowed from thermodynamics to describe disorder, plays a crucial role in the gradual degradation of security systems. Over time, without regular maintenance and updates, even the most robust security measures can fail. Imagine a fallen/cut fence or an outdated camera system that no longer captures clear images. These are tangible examples of how entropy impacts security. Furthermore, as threats evolve, our security measures must adapt. Old technologies and protocols have become less effective against modern threats, increasing the vulnerability of our systems. This natural decline in effectiveness, if not addressed, can lead to significant security breaches with direct outcomes on ratepayers. Action is expensive. Inaction costs a fortune.

Since the Cal Advocate's tour of SJWC facilities several months ago, a landscaper in a locked SJWC station doing work had two thieves climb over a fence and attempt to steal their truck and trailer. They got stuck on a berm at the fence line, which exemplifies the current condition that fences are easily penetrable and crime occurs inside our stations.

Attachment G, the confidential presentation to Cal Advocates details examples of threats against employees including gun violence, terrorist threats, trespassing, and others.

Conclusion

SJWC believes that the 8284 Physical Security submission provides the best sizing, lowest cost, and longest-lasting approach to physical security. Further, it is the most responsible for both the security of SJWC systems and the continuity of quality water service for our customers. SJWC requests the Commission to fund the requested GRC allocation of $5,054,900 for 2024, 5,275,300 for 2025, and 5,517,800 for 2026.

ATTACHMENT A

STATEMENT OF QUALIFICATION

SAN JOSE WATER COMPANY

STATEMENT OF QUALIFICATIONS

MARK HATCHER

My name is Mark Hatcher, and my business address is 1265 South Bascom Ave, San Jose, California 95128. I am currently serving as the Physical Security Manager at San Jose Water Company (SJWC), an investor-owned public utility and one of the most technically sophisticated urban water systems in the United States.

In my role at SJWC since March 2022, I have defined the physical security resources ecosystem, aligning over 100 elements with ASIS, ASCE, ANSI, and ISO standards. I have produced gap and process analyses using the Enterprise Security Risk Management (ESRM) maturity model, directed 75 site-specific physical security assessments, and developed 30 implementation site plans to a rough order of magnitude. My responsibilities also include managing OPEX and CAPEX security investments across over 195 locations, significantly improving the planning, budgeting, design, and commissioning of physical security measures. Additionally, I have implemented an enterprise Workplace Violence Program, conducted gap analyses and site vulnerability assessments, and developed active assailant protocols and mitigation response teams.

Before my current role, I served as a Lieutenant/Unit Commander at the Santa Clara County Office of the District Attorney. I directed the $2.4M design, construction, and operations of high-risk evidence facilities and managed a $1M+ campus-wide security project, enhancing employee and public safety through advanced security systems. I developed regional procurement requirements, co-authored a municipal privacy ordinance, designed an eDiscovery solution for 20 municipal organizations, and created a data-sharing platform for 130 first responder agencies. I also created a violent crime reduction methodology based on a criminal offender regressive statistical and logistics study. My efforts led to significant crime reduction and over 200 successful violent crime prosecutions in the first year of operation. I managed a Federal money laundering task force and authored economic espionage models for the Treasury Department and the intelligence community, including the CIA. Additionally, I held a Top Secret clearance while working for the National Security Division of the Federal Bureau of Investigation, FBI.

I managed worldwide intellectual property protection efforts and investigations at Intel Corporation. I also founded Innovative Homeless Solutions, a nonprofit focused on improving service delivery to the unhoused through data-centric approaches and advanced analytics.

I hold a Bachelor of Science degree in Criminal Justice from San Jose State University. My professional background includes extensive experience in physical security, law enforcement, and public administration, underscored by a commitment to leveraging data and technology to enhance operational efficiency and community safety.

I prepared documentation and testimony for the FY24-26 general rate case submission 5284 Physical Security.

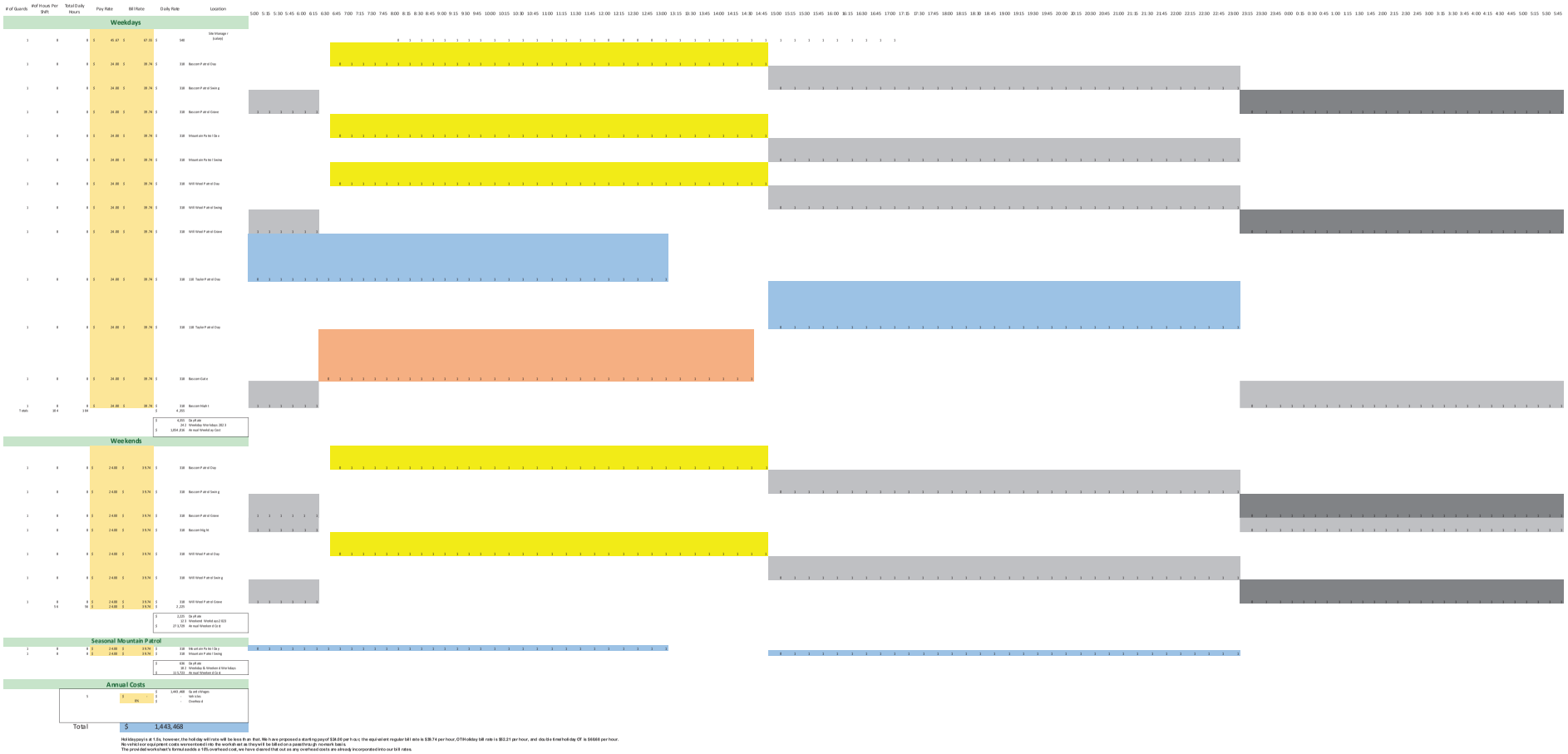
My diverse experience in physical security, law enforcement, and nonprofit leadership equips me with the skills and insights necessary to address complex security challenges and improve emergency management practices. My track record of successfully implementing security measures, reducing crime,

and enhancing community relations demonstrates my ability to contribute significantly to the safety and resilience of San Jose Water Company.

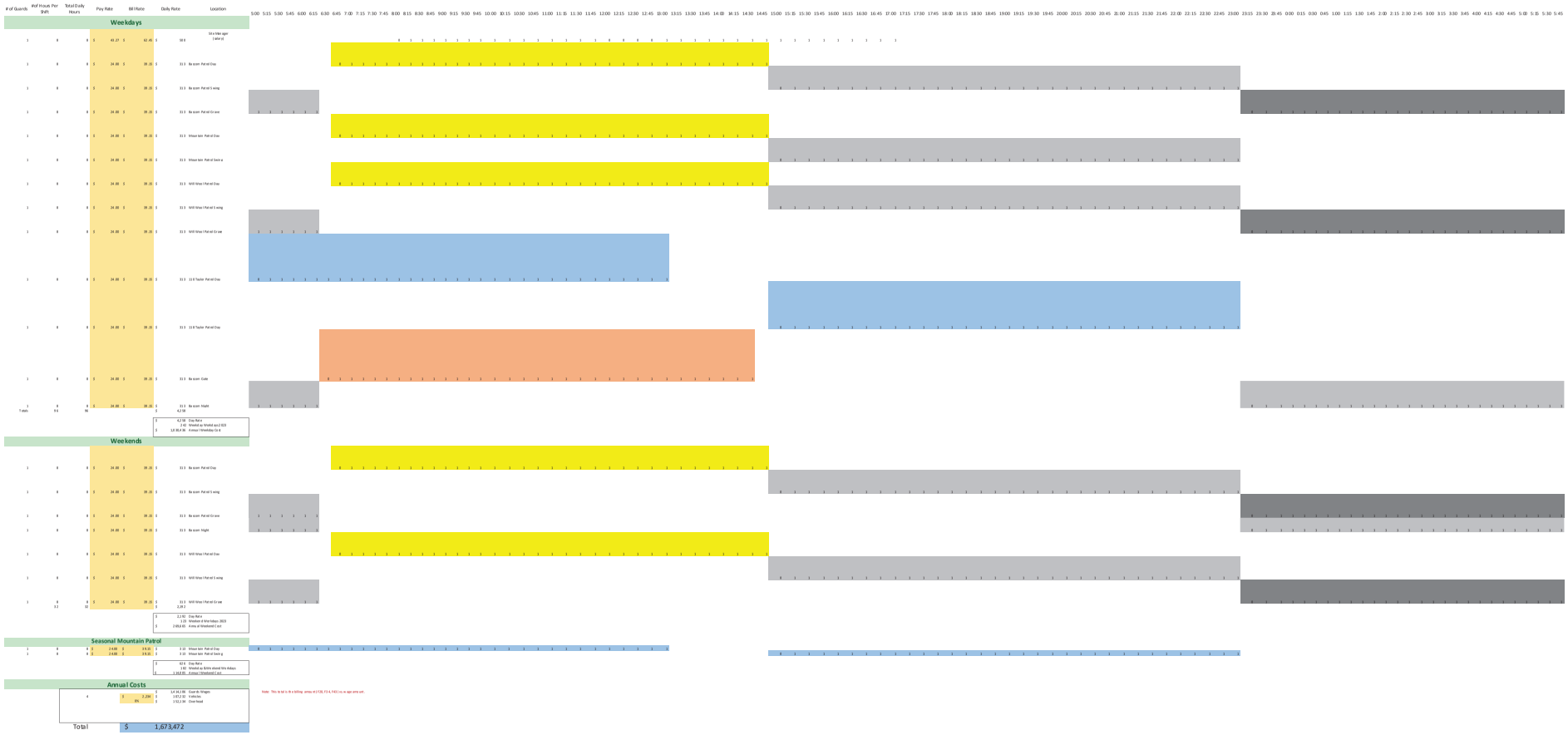
ATTACHMENT B

GUARD SERVICES RFI RESPONSES

ATTACHMENT B
1 of 2



ATTACHMENT B
2 of 2



ATTACHMENT C

MASSACHEUSETTS INSTITUTE OF TECHNOLOGY

LIVING WAGE STUDY

Living Wage Calculation for San Jose-Sunnyvale-Santa Clara, CA

The living wage shown is the hourly rate that an **individual** in a household must earn to support themselves and/or their family, working full-time, or 2080 hours per year. The tables below provide living wage estimates for individuals and households with one or two working adults and zero to three children. In households with two working adults, all hourly values reflect what one working adult requires to earn to meet their families' basic needs, assuming the other adult also earns the same.

The poverty wage and state minimum wage are for reference purposes. Poverty wage estimates come from the Department of Health and Human Services' Poverty Guidelines for 2024 and have been converted from an annual value to an hourly wage for ease of comparison. The state minimum wage data is sourced from the Labor Law Center and includes the minimum wage in a given state as of January of that year.

For further detail, please reference the Methodology page. The data on this page was last updated on February 14, 2024.

	1 ADULT				2 ADULTS (1 WORKING)				2 ADULTS (BOTH WORK		
	0 Children	1 Child	2 Children	3 Children	0 Children	1 Child	2 Children	3 Children	0 Children	1 Child	2 Children
Living Wage	$32.87	$58.25	$75.64	$98.31	$43.04	$51.16	$56.54	$63.11	$21.52	$31.18	$40.21
Poverty Wage	$7.24	$9.83	$12.41	$15.00	$9.83	$12.41	$15.00	$17.59	$4.91	$6.21	$7.50
Minimum Wage	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00	$16.00

Living Wage Benchmark Series

2024 Technical Documentation

Updated February 2024

About the Living Wage Institute

The Living Wage Institute is a benefit corporation founded in 2023, leveraging over 20 years of expertise from the creators of the Living Wage Calculator, a leading public resource for living wage data in the United States. Recognizing that today's employers are ready to design and implement their own living wage strategy, the Living Wage Institute works to equip them with the right data — like the Living Wage Benchmark Series — and insights to unlock better business performance and benefits to workers.

Overview

This technical documentation details the process by which by which the Living Wage Institute developed the Living Wage Benchmark Series (the Series) for 2024, which features highly localized living wage data across the United States. We leverage the most recent data from a variety of credible sources to calculate costs for eight basic needs plus income and payroll taxes at the county and metro levels, among other geographies, for 12 different family types. Together, these underlying costs help estimate the employment earnings — or the **living wage** — that a full-time worker requires on an hourly basis to cover the costs of their family's basic needs where they live while still being self-sufficient.

While there may be year-over-year variation in data sources and methods, the process for estimating a living wage broadly includes five core steps concerning: (1) Geographies, (2) Families, (3) Cost Components, (4) Calculation, and (5) Aggregation.

Geographies

Many labor market factors — like state and local taxes, market supply and demand, competition, logistics, shipping, seasons, microclimates, and climate risks — can impact the local costs of goods and services. In the United States, this localized variation is a key driver of communities' cost of living, and therefore, living wages. That's why the Series includes living wage estimates for all **3,143 counties and county equivalents** in the United States.

Counties — or their equivalents like Parishes in Louisiana or Boroughs in Alaska — are *legal/administrative entities* within each state for which the U.S. Census Bureau collects boundary information and tabulates data. The Census Bureau's county delineation file, which was last updated in 2020, serves as the base unit of geography for all our estimates. To remain compatible with the underlying datasets used to estimate a living wage, we do not use the newest county equivalent delineations for Connecticut, which only were fully integrated into Census Bureau datasets at the beginning of 2024.

Family types

In addition to counties, the Series is also segmented by **12 common family types** to account for the effect that family size has on the cost of basic needs. The family types are composed of varying numbers of working adults, non-working adults, and children, ranging from a single working adult with no children to two adults, one working, with three children. Because some costs — like food, childcare, and income and payroll taxes — vary depending on lifecycle stage, we make some general assumptions about each individual's age, too: The first child is 4; the second is 9; and the third is 15.

Cost components

For each family type across all 3,143 counties, we next collect data on the cost of *basic needs*. While there are many different interpretations of what should be included in the list of basic

needs, the Series takes inspiration from the foundational two tiers of Maslow's hierarchy (Physiological needs and Safety needs) to identify eight needs that when met, offer a minimum but adequate standard of living without reliance on public assistance. Together, eight basic needs – childcare, civic engagement, food, health care, housing, internet and mobile, transportation, and other necessities — make up the underlying cost components of the living wage. In the sections below, we describe the data sources, assumptions, and methods used to construct each of the eight cost components.

Childcare

Data on the cost of childcare primarily comes from the Department of Labor Women's Bureau's National Database of Childcare Prices, which includes county-level price data from state-run market rate surveys for childcare between 2008 and 2018. Though this data is available for the vast majority of counties in the United States, there are some areas with a high degree of missing data. We fill these gaps with state-level data from Child Care Aware of America's 2022 annual price of childcare report. To vary the Child Care Aware state data down to the county-level, we multiply them by a population-weighted index based on gross median rent data from the 2022 American Community Survey (5-Year Estimates).

Both the Women's Bureau and Child Care Aware datasets feature price data disaggregated by care types and age groups. Since there is limited data available on utilization rates of center- and home-based care in urban versus rural counties, we build our childcare cost estimates on the price of the center-based care type alone. We further assume the first child uses toddler care, the second uses preschool care, and the third child uses before/after school and two full-time months of summer care. This intentionally deviates from our standard age assumptions established earlier because childcare prices often underestimate the actual incurred *cost* of childcare to parents. We offset this potential underprediction by using the cost of childcare for younger children, which tends to be higher.

To ensure that all our final estimates for childcare are comparable to other cost components, we use the Consumer Price Index for all urban consumers for day care and preschool (CPI-U Series SEEB03) to adjust the data to December 2023 dollars.

Civic engagement

Data on the cost of civic engagement — or the ability to participate in your local community — comes from the 2022 Consumer Expenditure Survey. The Consumer Expenditure Survey is a national household interview and diary survey conducted annually by the U.S Bureau of Labor Statistics to quantify how consumers spend their money across different categories of goods and services.

The cost of civic engagement specifically is constructed by summing together the Consumer Expenditure Survey's annual expenditure means for audio-visual equipment; education; fees and admission; other entertainment; pets; reading; and toys, hobbies, and playground

equipment by the size of the consumer unit, which functions as a rough proxy for family size. We introduce further geographic variation to these otherwise national-level survey means by multiplying them by an index built from an average of these same goods and services categories by Census region of residence.

To ensure that all our final estimates for civic engagement are comparable to other cost components, we use the Consumer Price Index for all urban consumers for commodities generally (CPI-U Series SAC) to adjust the data to December 2023 dollars.

Food

Data on the cost of food comes from the U.S. Department of Agriculture's Monthly Cost of Food report estimate for June 2023. We specifically use data for the Low-Cost Food Plan, which tallies the national price of food in a market basket containing a nutritious and practical diet made from food purchased at a grocery store and prepared fully at home. Out of the four nutritionally adequate standards defined by the U.S. Department of Agriculture, the Low-Cost Food Plan is the second least expensive.

The report disaggregates monthly costs by age-sex group. To match these age-sex categories to the Series' standard age assumptions, we use the average cost between men and women age 19 to 50 for each adult; the cost of food for children age 4 to 5 for the first child; the cost of food for children age 9 to 11 for the second child; and the average cost between men and women age 14 to 18 for the third child. In a footnote, the U.S. Department of Agriculture also recommends applying a household size adjustment since their costs are calibrated for a household of four: The summed costs for family sizes other than four are further scaled by 1.20 for one person; 1.10 for two people; 1.05 for three people; and 0.95 for five people.

The Series introduces geographic variation using data from Feeding America's 2023 Map the Meal Gap — a public resource that measures food insecurity at the county-level — to account for local differences in food price. The dataset's cost per meal variable multiplies the national average meal cost for food-secure individuals by county-specific market basket prices for items in the U.S. Department of Agriculture's Thrifty Food Plan sourced from Nielsen. We construct an unweighted county-level index from this variable and apply it to our adjusted Low-Cost Food Plan cost estimates.

To ensure that all our final estimates for food are comparable to other cost components, we annualize them and use the Consumer Price Index for all urban consumers for food (CPI-U Series SAF1) to adjust the data to December 2023 dollars.

Health care

The cost of health care is composed of two subcategories in the Series: (1) premiums associated with employer-sponsored health insurance plans and (2) out-of-pocket medical expenses.

Health insurance premiums

Data on the cost of health insurance premiums comes from the 2022 Medical Expenditure Panel Survey Insurance Component (MEPS-IC). The Agency for Healthcare Research (a subdivision of the U.S. Department of Health and Human Services) and the U.S. Census Bureau fields the MEPS-IC on an annual basis to, in part, collect information about employer-sponsored health insurance from private employers and other entities. We use the MEPS-IC data tool to extract the state-level average employee contribution to health insurance plans among private sector establishments.

The data from MEPS-IC is grouped into three coverage categories that we attribute to different family types. We assume that a single adult with no children uses "single coverage"; two adults with no children use "employee plus one coverage"; and families with any number of children use "family coverage." These broad groupings, however, can result in underestimations of the employee contributions to health insurance premiums for larger family types.

We introduce county-level variation into the data by building an index with the Robert Wood Johnson Foundation and Ideon's HIX Compare. HIX Compare is a public resource that consolidates individual and small group insurance market information across all plan rating areas. These rating areas can be mapped back to counties. Using aggregated quarterly observations for small group silver plans in 2023, we calculate a county-level index within each state for individual and family premiums then apply the individual premium index to the data for single adults with no children and the family premium index to all other family types.

To ensure that all our final estimates for health insurance premiums are comparable to other cost components, we use the Consumer Price Index for all urban consumers for medical care (CPI-U Series SAM) to adjust the data to December 2023 dollars. We do not use the Consumer Price Index for health insurance (CPI-U Series SEME) because it excludes health insurance premiums.

Out-of-pocket medical expenses

Data on the cost of out-of-pocket medical expenses that are not covered by health insurance comes from the Bureau of Labor Statistics' 2022 Consumer Expenditure Survey. The cost of out-of-pocket medical expenses is calculated by adding together the survey's annual expenditure means for drugs, medical services, and medical supplies by the size of the consumer unit, which functions as a proxy for family size.

Since the Consumer Expenditure Survey medical expenses are at the national-level, we use an index based on the mean health care expenditure per person by Census region retrieved from the 2022 Medical Expenditure Panel Survey Household Component (MEPS-HC) data tool to introduce further geographic variation. Unlike the MEPS-IC, the MEPS-HC surveys households across the United States to, in part, collect data on usage of medical care and the costs incurred from it.

To ensure that all our final estimates for out-of-pocket medical expenses are comparable to other cost components, we use the Consumer Price Index for all urban consumers for medical care commodities (CPI-U Series SAM1) to adjust the data to December 2023 dollars.

Housing

Data on the cost of housing comes from the U.S. Department of Housing and Urban Development's 2024 Fair Market Rents, which features data released in October 2023. Fair Market Rents are estimates of the 40th percentile gross rent — including the cost of shelter, contract rent, and all major utilities sans telephone, cable or satellite, television, and internet services — for standard quality units. The U.S. Department of Housing and Urban Development typically uses these estimates to determine thresholds for federal housing assistance programs.

The Fair Market Rent data is disaggregated by unit size, ranging from zero (single occupancy, studio, or efficiency) to four bedroom apartments. We match these unit sizes to the minimum needs of each family type, assuming that a single adult with no children requires zero bedrooms; two adults with no children require one bedroom; families with one or two children require two bedrooms; and families with three children require three bedrooms.

We take a piecemeal approach to standardizing geographic variation since the Fair Market Rent data is available for Metropolitan Statistical Areas defined by the Office of Management and Budget, metro areas defined by the U.S. Department of Housing and Urban Development (HUD Metro FMR Areas), non-metropolitan counties, and some sub-county entities. For both types of metro areas, we introduce county-level variation by multiplying the rent estimates by a population-weighted county-level index within each metro area based on gross median rent data from the 2022 American Community Survey (5-Year Estimates). We use data for non-metropolitan counties as reported. And for the sub-county entities, we aggregate the data up to the county-level using a population-weighted mean.

To ensure that all our final estimates for housing are comparable to other cost components, we annualize them and use the Consumer Price Index for all urban consumers for housing (CPI-U Series SAH) to adjust the data to December 2023 dollars.

Internet & mobile

The cost of internet and mobile is composed of two subcategories in the Series: (1) home internet plans and (2) cellular telephone (mobile) service subscriptions. While the U.S. Department of Housing and Urban Development's Fair Market Rent estimates leveraged for the Series' housing cost component account for major tenant-paid utilities, it does not include internet and telephone services, both of which represent an increasing expense to families across the country.

Internet

Data on the cost of home internet plans comes from BroadbandNow's United States County Broadband Statistics for 2020 report released in November 2023. BroadbandNow sources county-level data on the price of lowest-cost monthly plans primarily from the Federal Communications Commission and the U.S. Census Bureau, filling in gaps with proprietary data from Internet Service Providers (ISPs).

Because internet service is a household-wide utility, we assume that all family types pay for only one plan regardless of their size. And though data is available for almost all counties across the United States, because BroadbandNow's dataset pulls from an older county delineation file, we use the state average lowest-cost monthly plan price for a handful of new counties missing data.

To ensure that all our final estimates for internet service are comparable to other cost components, we annualize them and use the Consumer Price Index for all urban consumers for internet services and electronic information providers (CPI-U Series SEEE03) to adjust the data to December 2023 dollars.

Mobile

Data on the cost of cellular telephone (mobile) services comes from the Bureau of Labor Statistics' 2022 Consumer Expenditure Survey.

The cost of mobile service expenses is calculated from the survey's annual expenditure means for cellular phone service by the size of the consumer unit, assuming that only adults in the family use this utility. We introduce further geographic variation to this national-level data by multiplying them by an index built from the mean cellular phone service expenditure by Census region of residence.

To ensure that all our final estimates for mobile services are comparable to other cost components, we use the Consumer Price Index for all urban consumers for wireless telephone services (CPI-U Series SEED03) to adjust the data to December 2023 dollars.

Transportation

Data on the cost of transportation comes from the 2019 Housing & Transportation Index (H&T Index), which was most recently updated in 2022. The H&T Index is maintained by the Center for Neighborhood Technology and, in part, includes an estimate for total transportation costs across all counties in the United States built from modeled data on auto ownership, auto use, and transit use.

We specifically use the estimated total transportation costs for a regional moderate household — defined as the typical household earning 80% of the area median income — as a base. To transform the transportation cost from a household figure to an estimate for a single commuter, we attenuate the total cost by the ratio of total workers age 16 and over to total

workers age 16 and over who do *not* work from home. This state-level ratio comes from data in the 2022 American Community Survey (5-Year Estimates).

The rebased transportation cost data is then multiplied by a family size-weighted index built from the 2022 Consumer Expenditure Survey annual expenditure means for used cars, gasoline, other vehicle expenses, and public transit by size of the consumer unit.

To ensure that all our final estimates for transportation are comparable to other cost components, we use the Consumer Price Index for all urban consumers for transportation (CPI-U Series SAT) to adjust the data to December 2023 dollars.

Other necessities

Data on the cost of other necessities that are not covered by other cost components comes from the Bureau of Labor Statistics' 2022 Consumer Expenditure Survey.

The cost of other necessities is calculated from the survey's annual expenditure means for apparel; household furnishings and equipment; housekeeping supplies; personal care products; and miscellaneous household equipment by the size of the consumer unit, which functions as a rough proxy for family size. We introduce further geographic variation to these otherwise national-level survey means by multiplying them by an index built from an average of these same goods and services categories by Census region of residence.

To ensure that all our final estimates for other necessities are comparable to other cost components, we use the Consumer Price Index for all urban consumers for commodities generally (CPI-U Series SAC) to adjust the data to December 2023 dollars.

Calculation

The Series computes county-level living wage estimates for all 12 family types, drawing on the data collected for the eight cost components to first simulate the rough effects of income and payroll taxes on the family's budget and then determine the hourly earnings that each working adult would need to earn to meet their basic needs. In the sections below, we describe the steps by which our living wage estimates are calculated.

Sum all cost components

For all 3,143 counties across the 12 family types, we add together all of the cost component estimates, using the following formula:

```
Basic needs budget (after tax) = (Childcare + Civic
engagement + Food + Health care + Housing + Internet &
mobile + Transportation + Other necessities)
```


This sum results in an annual basic needs budget *after* taxes have been paid. It does *not* include the amount a family would need to withhold from their earnings to be able to cover their tax burden.

Simulate the additional cost of income and payroll taxes

To account for the additional expense associated with income and payroll taxes, the Series leverages the National Bureau of Economic Research's TAXSIM (v35). TAXSIM is a microsimulation program that uses 35 input parameters and information about the federal and state income and payroll tax system to model personal tax liabilities.

For ease of computation, we assume that family types with one adult file as the head of household and those with two adults are married and file jointly. Our standard assumptions for family types further determines the age and number of dependents in the household. The basic needs budget after taxes is used as an input for wages, split equally between the total number of working adults in the family. And the county helps identify the state of residence to apply the appropriate statutory tax rate. We also consider rent paid and child care expenses as part of our inputs. All other input fields are set to zero.

Based on these inputs, the TAXSIM model outputs a rough estimate for federal income tax, state income tax, and the Federal Insurance Contributions Act (FICA) payroll tax liability for each observation in the Series. Since employers cover half of the FICA liability, we only include the portion contributed by the worker, or 7.65% (with 6.2% going to Social Security and 1.45% going to Medicare). These outputs are factored back into to the basic needs budget after tax, using the following formula:

```
Basic needs budget (before tax) = Basic needs budget (after
tax) + [Basic needs budget (after tax)*(federal income tax
 rate) + Basic needs budget (after tax)*(state income tax
rate) + Basic needs budget (after tax)*(0.5*FICA tax rate)
```

This yields an annual basic needs budget *before* taxes — in other words, the total annual budget a family requires to meet all their basic needs, including taxes.

It's important to note that because the TAXSIM model estimates a family's tax burden based on the sum of the cost components (and not on actual income) , our value for the cost of taxes may be underestimated.

Divide by the number of working adults

Next, the annual basic needs budget before taxes is divided by the total number of workers in a given family type, as demonstrated in the formula below:

```
Basic needs budget (before tax) per worker = [Basic needs
     budget (after tax) + [Basic needs budget (after
tax)*(federal income tax rate) + Basic needs budget (after
 tax)*(state income tax rate) + Basic needs budget (after
  tax)*(0.5*FICA tax rate)]] / number of working adults
```


For instance, if a family of four had two adults who both worked, the annual basic needs budget before taxes would be divided by two; however, if that family of four had two adults but only one worked, the annual basic needs budget before taxes would only be divided by one.

Calculate an hourly living wage

To translate what an individual worker must earn on an annual basis to meet their basic needs into an hourly living wage, we divide the annual basic needs budget before taxes by 2,080 hours, which assumes full-time work at 40 hours per week over 52 weeks per year.

```
Hourly living wage = [[Basic needs budget (after tax) +
[Basic needs budget (after tax)*(federal income tax rate) +
 Basic needs budget (after tax)*(state income tax rate) +
 Basic needs budget (after tax)*(0.5*FICA tax rate)]] /
        number of working adults] / 2,080 hours
```

This results in an hourly living wage estimate for all 3,143 counties across all 12 family types, the core variable of our Living Wage Benchmark Series.

Aggregation

Though our Living Wage Benchmark Series is primarily meant to be used at the county-level, we provide estimates for other geographies using county population estimates from the U.S. Census Bureau's 2022 American Community Survey (5-Year Estimates) to aggregate by a weighted mean.

These county estimates fold up into data for **384 Metropolitan Statistical Areas** (MSAs or metro areas) and **543 Micropolitan Statistical Areas** (μSAs or micro areas). The Office of Management and Budget delineates these *statistical areas*, which collectively make up Core Based Statistical Areas (CBSAs) characterized by counties in a populous urban nucleus surrounded by adjacent counties that also interact with that core. The standards for these delineations were last updated in 2020, with revisions announced in July 2023. As with counties, to prioritize data compatibility, we source our metadata for from the Census Bureau's 2020 CBSA delineation file.

For ease of reporting, we also produce estimates for other geographical units and the **nation** overall:

- **50 states and Washington, D.C.** State metadata comes from the Census Bureau's 2020 state delineation file.
- **9 divisions** and **4 regions.** These regions and their further subdivisions are groupings of states that are maintained by the Census Bureau. The latest metadata for these groupings comes from the 2022 regions and divisions delineation file.

ATTACHMENT D

AMERICAN SOCIETY OF CIVIL ENGINEERS

ASCE/EWRI 78-24

ASCE STANDARD

ASCE/EWRI

78-24

Guidelines for the Physical Security of Water and Wastewater/ Stormwater Utilities

ASCE
AMERICAN SOCIETY OF CIVIL ENGINEERS

EWRI
ENVIRONMENTAL & WATER RESOURCES INSTITUTE

ASCE STANDARD

ASCE/EWRI

78-24

Guidelines for the Physical Security of Water and Wastewater/ Stormwater Utilities

ASCE
AMERICAN SOCIETY OF CIVIL ENGINEERS

EWRI
ASCE

PUBLISHED BY THE AMERICAN SOCIETY OF CIVIL ENGINEERS

Cataloging-in-Publication Data on file with the Library of Congress

Published by American Society of Civil Engineers
1801 Alexander Bell Drive
Reston, Virginia, 20191-4382
www.asce.org/bookstore | ascelibrary.org

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

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

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

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

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

Photocopies and permissions. Permission to photocopy or reproduce material from ASCE publications can be requested by sending an email to permissions@asce.org or by locating a title in ASCE's Civil Engineering Database (https://cedb.asce.org) or ASCE Library (https://ascelibrary.org) and using the "Permissions" link.

Errata: **Errata, if any, can be found at http://dx.doi.org/10.1061/9780784485071.**

ISBN 978-0-7844-1615-0 (soft cover)
ISBN 978-0-7844-8507-1 (PDF)

Manufactured in the United States of America.

29 28 27 26 25 24 1 3 2 4 5

ASCE STANDARDS

The Board of Direction approved revisions to the ASCE Rules for Standards Committees to govern the writing and maintenance of standards developed by ASCE. All such standards are developed by a consensus standards process managed by the ASCE Codes and Standards Committee (CSC). The consensus process includes balloting by a balanced standards committee and reviewing during a public comment period. All standards are updated or reaffirmed by the same process at intervals between five and ten years. Requests for formal interpretations shall be processed in accordance with Section 7 of ASCE Rules for Standards Committees, which are available at https://www.asce.org/-/media/asce-images-and-files/publications-and-news/publications/documents/asce-rules-standards-committees.pdf.

Errata, addenda, supplements, and interpretations, if any, for this standard can also be found at https://ascelibrary.org/.

The provisions of this standard are written in permissive language and as such offer the user a series of options or instructions but do not prescribe a specific course of action. Significant judgment is left to the user.

This standard 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 standard by ASCE is not intended to warrant that the information contained therein is suitable for any general or specific use, and ASCE takes no position respecting the validity of patent rights. Be advised that the determination of patent rights or risk of infringement is entirely the user's own responsibility.

This page intentionally left blank

CONTENTS

This page intentionally left blank

PREFACE

Historically, malevolent acts have largely been categorized as threats alongside of natural hazards as part of an "All-Hazards" approach, and most vulnerability assessments score physical security as a low priority due to a lack of frequentist probability data when compared to natural weather phenomena. This has caused reduced confidence among owners and operators in the assessments and the subsequent mitigation steps for malevolent acts. Instinctively sensing something awry, key stakeholders have been likely to overspend on physical security countermeasures by trying to ensure the protection of everything, or conversely, by trusting that the assessment accurately revealed that security spending should be minimized, they grossly underspend. In this context, the ANSI/ASCE/EWRI 56-10/57-10 *Guidelines for Physical Security for Water and Wastewater/Stormwater Facilities* became little more than a checklist of optional security countermeasures without providing a means of cost–benefit analysis.

The suggested new direction was to update *Guidelines for the Physical Security of Water Utilities and Wastewater and Stormwater Utilities*, accepted in 2010 by ASCE. This new direction recognizes that the original intent of these guidelines was to serve as a "centralized starting point for water and wastewater/stormwater utilities to integrate modern security practices into the management, operation, construction, or retrofit of water, wastewater and stormwater systems."

Key Findings of 2021 ASCE/EWRI WISE SC Ad Hoc Group In 2021, the ASCE/EWRI WISE SC Ad Hoc Group indicated that previous versions of water sector security guidelines were limited, using a common risk model to protect against malevolent attacks. The original risk model was assessed in terms of threat likelihood, vulnerability, and consequence ($R = T \times V \times C$), which has led to a reaction of chasing threats, real or otherwise, and over- or under-hardening of critical assets as a reaction to the data produced. The reason is that defining a malevolent threat is dependent on the identification of the "who," "capability," and "likelihood" of malevolent actors, all of which were unknowns.

1. WHO: In an effort to define who the adversary might be, a prerequisite was placed on determining one of the predefined malevolent actor types of vandals, criminal, saboteur, or insider, also known as design basis threat (DBT) methodology. This resulted in a low probability of accuracy because of limited historical data. This approach also restricted the ability to guard against emerging threats such as foreign or domestically activated disenfranchised people groups through social media disinformation campaigns resulting in ground swell, organic attacks that do not fit in the DBT classifications. For these reasons, the use of DBT in these standards has been deprecated.
2. CAPABILITY: In addition, the effort was to define malevolent actor capability by presupposing their training, funding, ideology, preferred targets, tools, or ability to gain access to intelligence such as insider information, all without being caught by law enforcement. Again, limited historical data reduced this effort to guesswork, resulting in unfounded predictions about the preparation or skill a malevolent actor might have.
3. LIKELIHOOD: Likelihood of a malevolent threat event happening was calculated by using historical frequency. By following this method, the Environmental Protection Agency (USEPA) in February 2021 determined that out of 100,000 potential water utility targets, the likelihood of threat events such as adversaries jumping from helicopters into a water utility each year was 1:1,000,000 (or 10^{-6} power) (USEPA 2021). Using this approach for breach scenarios and data configurations has created wide error bands since the implied conclusion is to minimally invest in physical security countermeasures altogether.

The ASCE/EWRI WISE SC Ad Hoc Group indicated that the lack of an adequate data set from which to ascertain the aforementioned criteria put disqualifying limitations on the risk formula and created errors for making informed decisions. Furthermore, the attempt to derive meaningful data from what is not known has produced erroneous probability results that are hazardous to the physical security of water sector utility operations.

Cumulative Defense Strategy Overview Cumulative Defense Strategy is a process that is used to help secure critical assets against malevolent attacks. The process takes a wholistic approach to helping protect the facility under evaluation. Similar to methodologies used by other organizations, the approach considers the consequence of a particular critical asset being compromised and the approach used to carry out the attack. Using path analysis and the existing physical security countermeasure installed at the facility, the degree of difficulty to compromise the critical asset is mathematically calculated using the Foster–Wallace Formula (Wallace and Foster 2021). With this information, the facilities' vulnerability to different attack scenarios can be evaluated, response plans can be formulated, and subsequent risk management decisions can be made to further mitigate the current exposure in the event of an attack.

Mathematical Analysis of Defense Strategy and Countermeasures Methodology Overview The Mathematical Analysis of Defense Strategy and Countermeasures (MADSC) methodology is the process of evaluating the probability of success of a given threat based on a scenario identified, difficulty identified, and a consequence identified. It relies on cumulative defense strategy for the sequential increase in quantity and quality of physical security countermeasures across multiple defense layers to defend against specific attack vectors. Only attack vectors that are reasonable to defend against using security countermeasures available to the public sector are considered in these standards. The MADSC methodology as suggested by Wallace et al. (2024) provides a comprehensive plan to evaluate and enhance physical security countermeasures to defend against malevolent attacks.

Other Valuable ASCE Books Topics in *Structural Design for Physical Security*, MOP 142, could be a valuable resource to projects that have physical security concerns related to explosive, ballistic, forced entry, and hostile vehicle threats that include

- Threat determination and available assessment and criteria documents,
- Methods by which structural loadings are derived for the determined threats,

- Function and selection of structural systems,
- Design of structural components,
- Function and selection of window and facade components,
- Specific considerations for retrofitting structures,
- Testing methodologies, and
- Bridge security.

Additional topics in *Hazard-Resilient Infrastructure Analysis and Design*, MOP 144, provide a comprehensive description of facility resilience with respect to critical infrastructure. The process discussed in that MOP used in conjunction with the MADSC methodology could help provide a comprehensive hazard-resilient infrastructure plan for critical infrastructure.

ACKNOWLEDGMENTS

These voluntary guidelines were developed during the USEPA WISE Project, Phase 3, under the direction of the ASCE/EWRI WISE Standards Committee (ASCE/AWWA/WEF 2006a, b). The former committee consisted of the individuals first listed below through the end of the 2010 Committee balloting processes. The current ASCE/EWRI WISE standards committee consists of both groups of individuals listed.

Clyde R. Dugan
John H. Easton, Ph.D., *Vice Chair*
Conrad G. Keyes Jr., Sc.D., P.E., P.S., D.WRE (Ret.), Dist.M.ASCE, *Past Chair*
Jorge A. Garcia, Ph.D., P.E.
Neil S. Grigg, Ph.D., P.E., D.WRE (Ret.)
C. Dale Jacobson, P.E., BCEE, D.WRE
Charles R. Stack, MPH, BCES
C. Wesley Strickland, Esq.
James F. Wheeler, P.E.
Robert C. Williams, P.E., BCEE

The newest members listed per Fiscal Years 2020–2023 WISE SC balloting processes follow.

David Wallace, M.ASCE, *Chair*
Kris Schartau, B.S.E.E, A.M.ASCE, *Secretary*
Joseph Crisologo, P.E.
Thomas DeFelice, Ph.D., M.ASCE
Robert Janke
Kathlie S. Jeng-Bulloch, Ph.D., P.E., D.WRE, CFM
Leonard J. Kusek
David Lewin

This page intentionally left blank

CHAPTER 1
OVERVIEW OF GUIDELINES

1.1 SCOPE

The first physical security of water and/or wastewater/stormwater guidelines were developed as a joint effort between ASCE and the American Water Works Association (AWWA) with technical input from the Water Environment Federation (WEF), in accordance with ASCE Rules for Standards Committees, and were published initially as the proposed drafts, *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA/WEF 2006a) and *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006b). That consensus process included balloting by a balanced ASCE/Environmental & Water Resources Institute (EWRI) Water Infrastructure Security Enhancement (WISE) Standards Committee (SC) and reviewing during a public comment period. In 2014, Supplement No. 1 for the two ANSI/ASCE/EWRI physical security standards 56 and 57 were taken through the same process. From 2018 to 2021, another balloting process of combining the two documents (called Com 56-57 by the WISE SC) was taken through the last ASCE balloting process in 2021 and both 56 and 57 (ASCE 2010b, c) were withdrawn as ANSI/ASCE/EWRI standards; but the material was saved by the WISE SC and has become a part of these current guidelines. The provisions of this document have been written in permissive language and, as such, offer the user a series of options or instructions but do not prescribe a specific course of action. Significant judgment is left to the user of these documents.

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

1.2 PURPOSE OF THE GUIDELINES

These guidelines apply to the evaluation and enhancement of physical security for facilities used in potable water sources (raw water), treatment, and distribution systems, as well as for wastewater and stormwater facilities.

1.3 BACKGROUND OF THE INITIAL DEVELOPMENT

Highlights related to the creation of all the WISE guidance documents and/or standards in the early years of the twenty-first century are summarized as follows (ASCE 2010b, c; Wallace et al. 2024):

1. Under the US 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 of their water systems. The vulnerability assessments often recommended security improvements to reduce the risk of malevolent acts (such improvements may also reduce the risk associated with natural events). Similar requirements for wastewater utilities have yet to be promulgated, but the protection of wastewater utility facilities using similar approaches has been promoted by the Environmental Protection Agency (USEPA) and various industry organizations. In addition, ASCE, AWWA, and WEF agreed to work together to develop materials to assist in the implementation of security recommendations and the overall improvement of water and wastewater infrastructure security. The project was funded by USEPA under a cooperative agreement to foster public/private partnership in water and wastewater security. This project was known as the USEPA Water Infrastructure Security Enhancements (WISE) Project.
2. Phase 1 of the USEPA WISE project focused on the creation of Interim Voluntary Security Guidance documents (ASCE/AWWA/WEF 2004a, b, c). 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.
3. Under the direction of the EPA, Phase 3 focused solely on the development of physical security guidelines for water, wastewater, and stormwater facilities. These voluntary consensus guidelines were first developed as the Draft and were published initially as *Guidelines for Physical Security for Water Utilities* (ASCE/AWWA/WEF 2006a) and *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006b).
4. The USEPA Water Security Working Group presented its report *Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on Water Security Practices, Incentives, and Measures* to the National Drinking Water Advisory Council (NDWAC) on May 18, 2005 (WSWG 2005). Those findings included 18 features of an "active and effective" security program. The ANSI/ASCE/EWRI 56 and 57 guidelines addressed the following NDWAC recommendations, which discussed 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.

5. In 2011, the proposed update to *Guidelines for the Physical Security of Water Utilities and Wastewater and Stormwater Utilities* was accepted by ASCE to match more closely what has become accepted as standard industry practice in the J100-10 and G430-14. The updates to ASCE 56-10 and 57-10 maintained the DBT approach to characterizing malevolent threats and determining threat likelihood while the J100-10 focused on an "All-Hazards" approach to determining threat likelihood. AWWA (2013) further stated that identifying these threats was only possible with the use of "available intelligence." Malevolent acts and random natural weather events were summarized into design basis threats according to Mandatory Appendix E, RAMCAP Reference Threats in the J100-10(R13) document (AWWA 2013). Since malevolent acts have largely been categorized as threats alongside natural hazards as part of an "All-Hazards" approach, most assessment models score physical security as a low priority due to a lack of historical frequency data.

1.4 USE OF THESE GUIDELINES

The major points for the use of this standard (ASCE 2010b, c; Wallace and Foster 2021) imply that

1. It is the responsibility of the user of an ASCE/EWRI standard or guideline to determine that the products and approaches described in the standard or guideline are suitable for use in the application being considered.
2. To effectively use the standard or guideline, a water utility should first familiarize itself with the contents of this document. The Preface, Chapter 2, and Chapter 3 cover key concepts and terms that will help guide water utilities in creating nonoffensive defense strategies to help defend their facilities against malevolent attacks. Appendix B contains countermeasure reference tables designed to assist with the analysis process. It is recommended that water utility operators be knowledgeable and maintain security awareness about all the critical asset locations within the facility. This will help provide a foundation for following the cumulative defense strategy process flow chart detailed in Chapter 2.
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 new direction of the WISE SC members. The physical security countermeasures 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. This document contains instructions that describe the basic steps for its use. The guidelines also contain information that utilities should consider when applying the overall analyses to their specific facilities and needs.
4. The water facility guidelines contain information that utilities should consider when applying specific security technologies and methods to individual facilities or assets. The Preface, Chapter 2, Chapter 3, and the appendixes contain foundational information that is applicable to all water, wastewater, and stormwater utility types. 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 utility or critical asset.

1.5 GLOSSARY AND ABBREVIATIONS

Access Control: 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

Adversarial Use of Maritime Vehicles: Adversary attempting to gain access, incapacitate, disrupt, or destroy the facility using various watercraft devices

Adversarial Use of Unmanned (Uncrewed) Aerial Systems (UAS): Can be used to deliver payloads to conspicuous locations that would remain hidden for extended periods of time; the payload could include radio frequency jamming and data sniffing equipment, surveillance equipment, or weaponization.

Adversary: Anyone or anything used to attempt to gain access, incapacitate, disrupt, or destroy the facility

Adversary on Foot (AOF): Anyone attempting to gain access to, incapacitate, disrupt, or destroy the facility using their own mobility

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

ASDWA: Association of State Drinking Water Administrators

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

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

Attack Vectors: Method by which an attack is carried out against a facility. Attack vectors include Adversary on Foot (AOF), Vehicle Ramming/Breach (VR/B), Vehicle-Borne Improvised Explosive Device (VBIED), Unmanned (Uncrewed) Aerial Systems (UAS), Maritime Attack, and Cyber Attack.

AWWA: American Water Works Association

AwwaRF: Formerly the American Water Works Association Research Foundation, now called the Water Research Foundation

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

CCTV: Closed-circuit television

Characteristics of Countermeasures: Characteristics that describe the contribution of each countermeasure in defending the critical asset. Countermeasures are specifically selected for the defense layer element based on these characteristics. Effective physical security systems balance the following six characteristics: deter, detect, observe, delay, deny, and/or respond.

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

Clear Zone: 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

Consequence Identification: Anything that incapacitates, disrupts, or destroys the facility or compromises the water quality

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

Cost–Benefit Analysis: Helps determine which countermeasures provide the most benefit for the cost required to achieve an acceptable level of risk

Countermeasure: Reaction to or a defense against a hostile action to deal with a threatening situation

Criminal: Individual whose primary motivation 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.

Critical Asset: Any section or subsection of a facility that if compromised would result in degradation or full disruption of the water supply, water quality, or public safety issue

Critical Asset Identification: Process or method of ascertaining type of facility, level of redundancy, population served as well as critical assets of the facility and where they are physically located

Critical Asset Ingress: Access points that lead directly to the critical asset located within the facility

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

Cumulative Defense Strategy (CDS): Process by which physical and electronic security countermeasures are strategically installed in combination with defense layers to oppose specific attack vectors

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

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.

Defense in Depth: Application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another (ANSI/ISA 2007).

Defense Layer: Combination of countermeasures specifically designed as an affront to a specific path chosen by an adversary seeking to incapacitate, disrupt, or destroy a community water system

Defense Layer Element: Ordinal steps an adversary must cross to effect compromise; these steps are ordinal in that they must be crossed sequentially by an adversary to reach the final target.

Delay: Characteristic applied to any countermeasure that is used for extending the length of time required for the adversary to progress

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 used in multiple layers to provide protection in depth. Delay features are only effective when placed within a layer of detection.

Delta Difficulty: Calculated difference between two sequential countermeasure cumulative difficulty values

Deny: Characteristic applied to any countermeasure that is used to create controlled access and authorized user levels to the critical asset

Detect: Characteristic applied to any countermeasure that is used for creating awareness of someone or something that has crossed a line leading to a critical asset

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 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.

Detection Line: Point at which someone or something is detected within the perimeter of the facility

Deter: Characteristic applied to any countermeasure that is used to dissuade the occurrence of a low-level attack

Deterrence: Security countermeasures 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 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.

Difficulty Identification: Analyzes the existing countermeasures in each defense layer for the minimum difficulty threshold required to protect the critical asset and uses the Foster–Wallace formula to calculate the degree of difficulty to compromise the countermeasures installed to defend against specific attack vectors

DOD: Department of Defense of the United States

DVD: Digital versatile disc, digital video disc

EFI: Electronic frequency interference

Enhanced: Augmented with improved, advanced, or sophisticated features

EOC: Emergency operation center

EOL: End-of-line

EPA: US Environmental Protection Agency

EWRI: Environmental & Water Resources Institute of ASCE

Facility Exterior Ingress: Ingress points at the facility exterior that must be crossed to reach the critical asset. Common facility exterior ingress points include doors, windows, roof hatches, ventilation ducts, or vault covers. The facility exterior establishes the first layer of countermeasures with real stopping power against an attack such as steel doors and hardened windows.

Facility Interior: Includes all secondary ingress points leading up to the critical asset ingress. It is recommended that the layout of the secondary ingress points create choke points restricting access to critical assets. Some common secondary ingress points could include doors, windows, elevators, ventilation ducts, and drop ceilings.

Foot-Candle: 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

Ground Radar: Use of high-frequency radio waves reflected off a distant object to determine its position, velocity, or other characteristics in a security application

GSA: US General Services Administration

Harden: To improve the physical strength of a protective countermeasure

IESNA: Illuminated Engineering Society of North America

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

Information Technology Room: Room, closet, or rack in a facility typically dedicated to housing information technology equipment including but not limited to servers, switches, and routers

Insider: Individual who is granted normal access to a facility; this may be an employee, contractor, custodial worker, or authorized visitor.

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

IP: Internet Protocol

IR: Infrared

IT: Information Technology

K-rated: Indicates the Department of Defense certified barrier speed rating's maximum vehicle impact speed achieved when a vehicle traveling at normal speed is successfully arrested by the barrier from a perpendicular direction

Key Card Reader/Access: Entry to a facility via a device used by an individual or individuals

kHz: Kilohertz

lb: Pound

Long-Range Acoustic Device (LRAD): Provides the ability to communicate clearly over long distances with sound pressure levels capable of rising above the surrounding noise levels

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

Lux: 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

Mathematical Analysis of Defense Strategy and Countermeasures (MADSC) Methodology: Process of evaluating the probability of success of a given threat based on a scenario identified, difficulty identified, and a consequence identified. It relies on cumulative defense strategy for the sequential increase in quantity and quality of physical security countermeasures across multiple defense layers to defend against specific attack vectors. Attack vectors that are reasonable to defend against with security countermeasures available to the public sector are considered in these standards. The MADSC methodology provides a comprehensive plan to evaluate and enhance physical security countermeasures to defend against malevolent attacks.

MHz: Megahertz

Minimum Difficulty Threshold (MDT): Incremental increase in the quantity and quality of security countermeasures at each defense layer element required to protect the critical asset. The minimum difficulty threshold establishes the minimum number of countermeasures and the countermeasure characteristics required for each ordinal step.

NACWA: National Association of Clean Water Agencies [formerly the 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

Observe: Characteristic applied to any countermeasure used for maintaining visual awareness through optics, thermal, or radar capability

Observation Zone: Space between the detection line and the facility exterior. The purpose of the observation zone is to assess a potential threat and initiate predetermined response protocols.

OD: Outside diameter

Ordinal Step: Categorized steps an adversary must cross to reach the critical asset

PACS: Physical Access Control System

Path Analysis: Analyzes all paths that an adversary could take to compromise the critical asset considering a set of known attack vectors and countermeasures installed to oppose the attack vectors

Perimeter: Establishes the legal demarcation by defining the boundaries of a facility

Personnel Gates: Allow employees to access a facility through the perimeter

PIR: Passive infrared

PL: Public law

PLC: Programmable logic controller

Probability of Success of a Given Threat ($P_{S|T}$): Probability that an adversary will compromise a critical asset based on a scenario identified, consequence identified, and the degree of difficulty to compromise the facility

Protection in Depth: Strategy of providing multiple layers of protective countermeasures, thereby requiring an adversary to defeat a system, travel to the next protective layer and defeat that system, and so forth until reaching the target. An example of protection in depth is the application of layers of protective countermeasures 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 ($lb/in.^3$)

PTZ: Pan, tilt, and zoom

Public Address (PA) System: Electronic system used to increase the apparent volume of an acoustic source typically used to communicate or convey important information

PVC: Polyvinyl chloride

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

Respond: Characteristic applied to a planned sequence of actions taken because of an attack

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

Response Evaluation: Evaluation of available options in conjunction with existing countermeasures to take actions against an adversarial attack

RF: Radio frequency

RFI: Radio frequency interference

Risk: Potential for realization of unwanted, adverse consequences to human life, health, property, or the environment. The quantitative or qualitative expression of loss 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.

Risk Acceptance: Acknowledgment that the risk of compromise is less than the cost required to mitigate the risk

Risk Management: To make an informed risk decision based on the calculated probability of success of a given threat, for a consequence identified, scenario identified, difficulty identified, response options, and cost to remediate; manage risk by mitigating or accepting consequences.

Risk Mitigation: Implementation of strategies to reduce or eliminate a threat, or the effects of a threat

RTU: Remote terminal unit

Saboteur: An individual typically motivated by political, doctrinal, or religious causes, although revenge may also be a motivation. This individual primarily uses 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.

Sallyports: Designed to create controlled entry for vehicles by using a two-gate system. The first gate is usually part of the exterior perimeter fence or wall. The second gate is part of a fortified area that is enclosed on all sides and is sized to accommodate the largest vehicle required to enter the facility. The fortified area is similar to a mantrap except for vehicles. The second gate offers a greater degree of controlled access to a facility by restricting vehicle tailgating and provides an opportunity for additional verification or inspection to pass through the second gate.

Scenario Identification: Type and method of attack carried out against a facility usually referred to as attack vectors

Sequential Countermeasures (SCM): Ordered sequence of countermeasures across all the defense layer elements with an assigned probability of success of a given threat based on the results from the Foster–Wallace Formula

SI: International System of Units

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

Staged Gates: *See* Sallyport

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

Surveillance: 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

SWTP: Stormwater treatment plant

Target: Term used synonymously with critical assets throughout this standard

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

Thermal Cameras: Detection and measuring of radiation in the infrared spectrum being emitted from an object with the use of thermographic cameras. These infrared imaging systems produce thermal video or still images (thermograms) using color differences to point out the various temperature points of an object from hot to cold levels. Because the amount of radiation increases with higher temperatures, warm spots will stand out from colder spots on the thermal image. Thermal imaging cameras do not need light to operate; they can detect objects in total darkness or in daylight.

UFC: Unified Facilities Criteria

UL: Underwriters Laboratory

UPS: Uninterruptible power supply

Vandal: Individual acting alone or in a group, unarmed and using spray paint to deface property or hand tools to inflict damage to utility assets

Vehicle-Borne Improvised Explosive Device (VBIED): Adversary attempting to gain access, incapacitate, disrupt, or destroy the facility using a vehicle as an improvised explosive device

Vehicle Gates: Allow vehicles to access the facility through the perimeter

Vehicle Ramming Breach (VRB): Occurs when an adversary attempts to gain access to, incapacitate, disrupt, or destroy the facility using a vehicle as a tool to breach the facility

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

VMS: Video Management System

VSAT: Vulnerability Self-Assessment Tool, available from the National Association of Clean Water Agencies (NACWA)

Vulnerability: 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): 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).

Vulnerability Determination: Vulnerability of a facility determined by subtracting 1 minus the degree of difficulty to compromise the countermeasure install to defend the facility against specific attack vector

WEF: Water Environment Federation

WISE: Water Infrastructure Security Enhancements

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

WRF: Water Research Foundation

WSWG: Water Security Working Group

WTP: Water treatment plant

WWTP: Wastewater treatment plant

CHAPTER 2
APPLICATION OF GUIDELINES

2.1 INTRODUCTION

These water and wastewater/stormwater utility guidelines recommend a cumulative defense strategy, described in Section 2.2, for physical and electronic security countermeasures designed to protect community water systems against several types of malevolent attacks. Adversaries may be known or unknown. Defense strategies and countermeasures are closely coupled with the vulnerabilities that would be exploited and the attack vector used for this purpose (Ko and Choo 2015). By establishing defenses against multiple types of worst-case reasonable attack vectors, the facility will be better prepared to address multiple threat scenarios.

2.2 CUMULATIVE DEFENSE STRATEGY

Cumulative defense strategy is the process by which physical and electronic security countermeasures (hereafter called security countermeasures or countermeasures) are strategically installed in combination with defense layers (Section 2.7) to oppose specific attack vectors (Section 2.5). These countermeasures are recommended to incrementally increase in quantity and quality throughout the scale of the facility requiring an escalation of an adversary's capability, while at the same time improving the cost to benefit ratio of the potential solution.

To better understand cumulative defense strategy, the components of defense strategy must be understood. Cumulative defense strategy includes classifying attack vectors and the defense layers that oppose them, the ordinal steps an adversary crosses to reach the critical asset, and the countermeasures with specific characteristics used within each defense layer element to defend against the attack. The flow chart shown in Figure 2-1 is the high-level cumulative defense strategy process outlined in this chapter. Following the cumulative defense strategy process provides a comprehensive and repeatable method to effectively evaluate the physical security at water utilities against specific attack vectors. The process also reveals where vulnerabilities exist and provides recommendations for physical security improvements. The process relies on what can be known about the quantity and quality of countermeasures to defend against specific attack vectors rather than attempting to characterize objectives, motives, and capabilities of the adversary. Transitioning away from a DBT perspective to a cumulative defense strategy perspective will help provide a stronger case for physical security improvements within the water sector (Wallace et al. 2024).

2.3 CRITICAL ASSET IDENTIFICATION

These guidelines cover water, wastewater, and stormwater facilities that are components of water systems and are under the control of the utilities. All water system facilities contain critical assets required to maintain operation. Overall impact to the water utility may vary. Table 2-1 lists the water and wastewater/stormwater facilities mentioned in ASCE (2010b, c). A simplified approach has been considered for these standard guidelines by not expanding on every facility type in subsequent chapters. Appendix C details the scope and mission of the water facilities listed in Table 2-1.

Multiple critical assets may be contained within each of these facility types. Determining specifically which assets are deemed critical is up to each facility owner/operator. For example, a remote pump station may only have one critical asset being the contents within the building itself. A large water treatment facility may have multiple critical assets at different locations around the property. In this scenario, each critical asset will require a separate analysis according to the process outlined in Figure 2-1. Critical judgment is necessary when considering which components of the facility are required for the plant to function properly and safely.

2.4 CONSEQUENCE IDENTIFICATION: CRITICAL ASSET BREACH

The consequence identification (Figure 2-1) of a malevolent attack would include anything that incapacitates, disrupts, or destroys the water and/or wastewater/stormwater system facilities, compromises the water quality, or jeopardizes public safety.

2.5 SCENARIO IDENTIFICATION: ATTACK VECTORS

Scenario identification (Figure 2-1) only addresses how malevolent attacks could be carried out against a facility. Attack vectors identify the method an adversary might use to carry out the attack, but it does not attempt to characterize the adversary (Wyss et al. 2011). Attack vectors are limited to approaches that can be detected and defended against by countermeasures that are available to the civilian sector. Attack vectors that are more extreme, such as an aircraft used as an offensive weapon, cannot be defended against by available civilian countermeasures. Attacks of this nature cannot be detected with enough warning to provide a meaningful response with a non-offensive defense (NOD) strategy. Therefore, attack vectors that are of a national security nature are deferred to the responsibility of the federal government to protect against. Some specific attack vectors may not apply to every facility. For example, considering a maritime attack against a facility that does not have a waterfront or shoreline approach is meaningless.

2.5.1 Adversary on Foot An adversary on foot is anyone attempting to gain access to, incapacitate, disrupt, or destroy the facility using their own mobility.

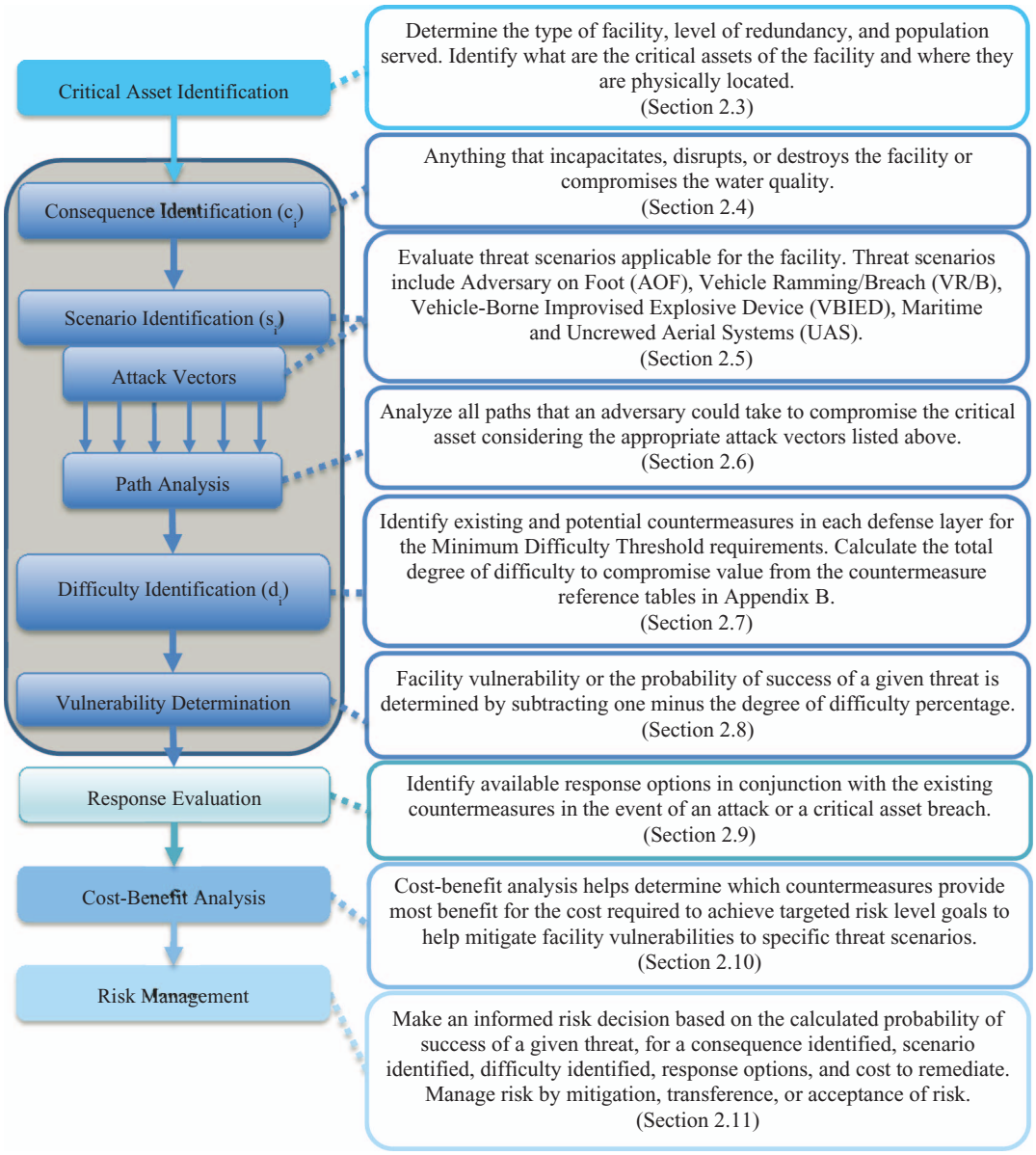


Figure 2-1. Cumulative defense strategy flow chart.

Table 2-1. Water System Facilities.

Water Facilities	Wastewater/Stormwater Facilities
C.1 Water Treatment Plants	C.7 Wastewater/Stormwater Treatment Plants
C.2 Raw Water Facilities	C.8 Collection Systems
C.3 Wells and Pumping Stations	C.9 Pumping Stations
C.4 Water System Support Facilities	C.10 Wastewater/Stormwater System Support Facilities
C.5 Finished Water Storage	
C.6 Water Distribution Systems	

2.5.2 Vehicle Ramming Breach A vehicle ramming breach occurs when an adversary attempts to gain access to, incapacitate, disrupt, or destroy the facility using a vehicle as a tool to breach the facility. Using mass and speed as a weapon, vehicles can cause severe damage to critical assets by crashing through perimeter fences and gates to reach the target to inflict maximum damage. Strategic placement of natural or man-made countermeasures with respect to the facility can significantly reduce the probability of a successful vehicle ramming breach attack.

2.5.3 Vehicle-Borne Improvised Explosive Device A vehicle-borne improvised explosive device involves an adversary attempting to gain access to, incapacitate, disrupt, or destroy the facility using a vehicle loaded with improvised explosive devices. The primary protection scheme against a VBIED attack is to maximize the distance between the facility and the vehicle. To achieve a protective distance from an explosion, kinetic energy–rated barriers known as *K-rated* bollards or boulders are recommended to be placed at all accessible locations around the facility. Existing facilities with established walk paths and parking lots could require significant modifications to achieve this level of protection. Bollard size, weight, and placement recommendations should come from qualified engineering and security professionals. Additional protection schemes against VBIED attacks can also include the fundamental design of the facility exterior, construction materials, and exterior hardening options.

2.5.4 Adversarial Use of Maritime Vehicles Adversarial use of maritime vehicles involves an adversary attempting to gain access to, incapacitate, disrupt, or destroy the facility using various watercraft devices. This type of attack vector is considered when the facility is physically located adjacent to a body of water or the facility could be breached directly from the water. Some potential forms of maritime vehicle attacks include personnel transport, ramming, clogging, diverting, or using improvised explosive devices.

2.5.5 Adversarial Use of Unmanned (Uncrewed) Aircraft Systems Adversarial use of unmanned (uncrewed) aircraft systems can be used to deliver payloads to conspicuous locations that would remain hidden for extended periods of time. The payload could include radio frequency jamming and data sniffing equipment, surveillance equipment, or weaponization.

2.5.5.1 Unmanned (Uncrewed) Aircraft System Surveillance Off the shelf uncrewed aircraft systems surveillance commonly includes high-definition video surveillance systems with live streaming and recording capability. This allows the adversary to surveil a particular target and gather intelligence about potential vulnerabilities from an inconspicuous location.

2.5.5.2 Unmanned (Uncrewed) Aircraft System Data Sniffing Adversaries can attach a radio frequency transmitter to uncrewed aircraft systems to disrupt existing wireless communications. When the disruption is removed, devices on the network retransmit their credentials to reconnect. The credentials are captured by a receiver on the uncrewed aircraft system and processed by the adversary to exploit vulnerabilities in the network.

2.5.5.3 Unmanned (Uncrewed) Aircraft System Weaponization Uncrewed aircraft system weaponization includes mounting firearms, explosives, chemical or biological agents, or other payloads, to the uncrewed aerial vehicle (Hernandez 2020). Adversarial use of these systems could allow an uncrewed aircraft system to travel to an unprotected location to inflict damage, gain access, incapacitate, disrupt, or destroy the facility.

2.6 PATH ANALYSIS

Path analysis (Figure 2-1) considers any route an adversary could take to reach the critical asset based on each attack vector scenario. Analysis of all defensible routes to critical assets are recommended for appropriate attack vector scenarios. Some of the routes could include going over an interior wall through a drop ceiling, breaking an unhardened window, or entering through an unsecured drainage pipe. Using critical judgment, one attempts to determine the path of least resistance to reach the critical asset. The presence or absence of countermeasures along the path establishes the degree of difficulty to compromise the critical asset. Appendix B contains multiple sets of sample countermeasure reference tables corresponding to each of the water system facility types. The tables in Appendix B are provided to establish a baseline for a minimum set of countermeasures based on the type and size of the facility. Select the appropriate countermeasure reference table from Appendix B and perform the path analysis based on the number of defense layer elements (Section 2.7.2) and attack vector scenarios.

2.7 DIFFICULTY IDENTIFICATION

Difficulty identification (Figure 2-1) analyzes the existing countermeasures in each defense layer based on the recommended minimum difficulty threshold required to protect the critical asset. The minimum difficulty threshold requires an incremental increase in the quantity and quality of security countermeasures at each defense layer element. The subsections of Section 2.7 describe the terminology used in cumulative defense strategy. Based on cumulative defense strategy the MADSC methodology (Wallace et al. 2024) is used to calculate the degree of difficulty to compromise the countermeasures by identifying all that would have to fail for a full critical asset breach. The degree of difficulty to compromise all the countermeasures is used to determine the probability of success of a given threat which is synonymous with facility vulnerability. Facility vulnerability is discussed in Section 2.8. Details on the difficulty analysis process are discussed in Chapter 3.

2.7.1 Defense Layer A defense layer is a combination of countermeasures specifically designed as an affront to a specific path chosen by an adversary seeking to incapacitate, disrupt, or destroy a community water system.

2.7.2 Defense Layer Elements Defense layer elements are the ordinal steps an adversary must cross to effect compromise. These steps are ordinal in that they must be crossed sequentially by an adversary to reach the final target.

2.7.2.1 Approach Zone The approach zone refers to the vehicle drive path area between the facility access gate and other access roads outside the property boundary. The configuration of this area helps determine the maximum vehicle approach speed prior to reaching the perimeter gate. Keeping vehicle approach speeds below a maximum acceptable threshold helps determine the size and type of K-rated barrier required to stop a vehicle ramming breach scenario.

2.7.2.2 Perimeter The perimeter establishes the legal demarcation by defining the boundaries of a facility. The perimeter typically consists of access points such as personnel gates, vehicle gates, and sallyports designed to deter access to the facility.

2.7.2.3 Personnel Gates Personnel gates allow employees and visitors to access a facility through the perimeter. It is recommended that all personnel gates have controlled access. Additional countermeasures with detection and observation capability are also recommended to facilitate screening of all individuals entering and exiting the facility.

2.7.2.4 Vehicle Gates Vehicle gates allow vehicles to access a facility through the perimeter. It is recommended that perimeter vehicle gates maintain the same level of deterrence capability as the perimeter fence. This is done to ensure that an adversary on

foot would have the same level of difficulty breaching the perimeter at any location. Like personnel gates, vehicle gates are recommended to have controlled access and additional countermeasures to provide screening capability.

2.7.2.5 Sallyports Sallyports (also referred to as secondary gates) are designed to create controlled entry for vehicles by using a two-gate system. The first gate is usually part of the exterior perimeter fence or wall. The second gate is part of a fortified area that is enclosed on all sides and is sized to accommodate the largest vehicle required to enter the facility. The fortified area is similar to a mantrap except for vehicles. The second gate offers a greater degree of controlled access to a facility by restricting vehicle tailgating and provides an opportunity for additional verification or inspection to pass through the second gate. Guard facilities along with dedicated personnel can be associated with sallyport entrances. Once both gates are closed and the vehicle is captured within the sallyport, a security guard may confirm the contents and driver authorization before releasing the vehicle.

2.7.2.6 Detection Line The detection line is the point at which someone or something is detected at or within the perimeter of the facility. In some cases, the detection line may not be located at the perimeter fence because installing a sensor to cover the entire fence line might not be cost effective. Early detection is important because it starts the clock for operators and security personnel to assess the situation in the observation zone and initiate a response.

2.7.2.7 Observation Zone The observation zone is defined as the space between the detection line and the facility exterior. The purpose of the observation zone is to assess a potential threat and initiate predetermined response protocols. Observation zone regions are typically established in these areas:

- Along the perimeter fence to allow for unobstructed surveillance of the fence area;
- Between a perimeter fence and structures, buildings, or other critical assets enclosed within the fence to maintain a clear area for detection; or
- Around the perimeter of a building to prevent areas of concealment.

Within the observation zone, prune, or trim vegetation to a height of 4 in. (100 mm) or less and remove large obstacles or rocks that can shield intruders from view.

2.7.2.8 Facility Exterior Ingress The facility exterior consists of ingress points that must be crossed to reach the critical asset. Common facility exterior ingress points include doors, windows, roof hatches, ventilation ducts, or vault covers. The facility exterior establishes the first defense layer with real stopping power against an attack by utilizing countermeasures such as steel doors and hardened windows.

Some facility exterior ingress points could be adjacent to public sidewalks, roads, or share a common wall with an unassociated building. In this scenario the facility exterior takes on the requirements of the perimeter, detection line, and observation zone. The detection line can be created with countermeasures thereby establishing an observation zone, but the distance aspect of the observation zone is significantly reduced or eliminated. This is more common in dense urban areas or where established infrastructure has been in place for a long time.

2.7.2.9 Facility Interior The facility interior includes all secondary ingress points leading up to the critical asset ingress. It is recommended that the layout of the secondary ingress points create choke points restricting access to critical assets. Some common secondary ingress points could include doors, windows, elevators, ventilation ducts, and drop ceilings.

2.7.2.10 Critical Asset Ingress The critical asset ingress point is typically the most difficult point of the entire facility to breach. It is recommended that the critical asset ingress point contains the most quantitative and qualitative countermeasures available to protect the critical asset. In a large water, wastewater, or stormwater treatment facility, a possible critical asset ingress point would be an interior door or window to an operations control room, IT room, SCADA closet, or chemical room. The critical asset ingress at a pump station could be the doors on the outside of the building. On a finished water storage tank, the critical asset ingress could be the vault hatch protecting the water.

2.7.3 Characteristics of Countermeasures The characteristics of countermeasures describe the contribution of each countermeasure in defending the critical asset. Countermeasures are specifically selected for the defense layer element based on these characteristics. Effective physical security systems balance the following six characteristics: deter, detect, observe, delay, deny, and respond.

2.7.3.1 Deter The deter characteristic applies to any countermeasure that is used to dissuade the occurrence of a low-level attack. Countermeasures with deter characteristics are not considered to have significant stopping power against attacks. These countermeasures include things like fencing, lighting, signage, surveillance equipment, or a clearly visible facility with no obstructions.

2.7.3.2 Detect The detect characteristic applies to any countermeasure that is used for creating awareness of someone or something that has crossed the detection line. Countermeasures with detection characteristics have no real stopping power but are necessary components to provide early warning of an attack. These countermeasures include things like security switch contacts, motion detectors, virtual trip wires, camera analytics, and ground radar.

2.7.3.3 Observe The observe characteristic applies to any countermeasure that is used for maintaining visual awareness through surveillance camera optics, thermal, or radar capability. Countermeasures with observation characteristics are designed to keep eyes on the target, track movement, and provide feedback to operators to help assess the situation. Images can be automatically queued up and recorded with an option to push the surveillance video to stakeholders and responders to track the situation remotely.

2.7.3.4 Delay The delay characteristic applies to any countermeasure that is used for extending the length of time required for the adversary to progress. Countermeasures with delay characteristics have real stopping power when it comes to preventing a critical asset breach. These countermeasures include things like steel doors, hardened glass, K-rated bollards, structural walls, trenches, and human capital.

2.7.3.5 Deny The deny characteristic applies to any countermeasure that is used to create controlled access and authorized user levels to the critical asset. Countermeasures with deny characteristics control the access points locking mechanisms from being actuated by unauthorized users. The quality of the access control countermeasure determines the degree of difficulty to compromise. Countermeasures such as encrypted PACS, dual-factor authentication, and/or multifactor authentication provide increasing levels of difficulty to deny access to the critical

asset. Access control systems that operate on a 125 kHz frequency, or keyed locks, are no longer considered to be controlled access because of their ease of duplication and compromise.

2.7.3.6 Respond The respond characteristic applies to a planned sequence of actions taken because of an attack. To effectively respond to an attack, detailed plans and procedures must be created so workers and operators know what to do when an attack occurs. In addition to the plans and procedures, countermeasures with response characteristics can be used to alert operators and stakeholders of the situation or communicate with the attacker that law enforcement is on the way. These countermeasures can include annunciators, strobe lights, and two-way audio communication equipment.

2.7.4 Importance of the Mathematical Analysis of Defense Strategy and Countermeasures Methodology The Mathematical Analysis of Defense Strategy and Countermeasures (MADSC) methodology moves past the prior attempts to accurately define threat likelihood and focuses attention on degree of difficulty to compromise the countermeasures by determining what would have to fail for adversarial compromise to be successful. Therefore, it should no longer matter who the malevolent actor is, what their capability is, historical frequency of attacks, or available intelligence. This method creates a meaningful path for investment considerations of physical and electronic security countermeasures for cost–benefit analysis and compensates for emerging threats such as domestically activated people groups (Wallace et al. 2024). Details about calculating the degree of difficulty to compromise the countermeasures are covered in Chapter 3.

2.8 VULNERABILITY DETERMINATION

Vulnerability determination is key to understanding where facility defenses are vulnerable to specific attack scenarios. Facility vulnerability (Figure 2-1) is determined by subtracting one minus the degree of difficulty to compromise percentage based on the MADSC methodology. Facility *vulnerability* is synonymous with the probability of success of a given threat. If the degree of difficulty to compromise all the countermeasures was calculated to be 75%, then the facility's vulnerability (or the probability of success of a given threat) would be 25%. Determining vulnerability percentages across multiple attack vectors can help contribute to the risk management discussion in Section 2.11.

2.9 RESPONSE EVALUATION

Response evaluation (Figure 2-1) involves examining the options available to determine the best course of action during an adversarial attack. Cumulative defense strategy enables the use of time as a tactical advantage to create a window of opportunity for emergency responders to arrive and interrupt the attack. In some situations, emergency responders may be delayed or unavailable to respond to an attack, so additional actions might be required to help protect the facility. Alternate responses could include switching to redundant sources to isolate the facility under attack or remotely disabling the facility to prepare for a total compromise. It is recommended that every utility develops response plans based on utility needs and support from their local law enforcement. Law enforcement intervention of an adversary's attack and apprehending the suspect prior to total compromise is the best option but is not necessarily reality. Attempting to maintain control of the facility for as long as possible to safely shut down critical systems is something that would ideally take place in a known amount of time. A facility shutdown to a safe predetermined state is important to help protect the public in the event of a full breach. If a shutdown is not possible, alternative response plans are recommended to ensure public safety.

2.10 COST–BENEFIT ANALYSIS

The cumulative defense strategy method also enables a consistency of approach by which mathematical analysis can be performed to determine the probability of success of a given threat and the evaluation of cost–benefit analysis (Figure 2-1). Defense strategy analysts can quickly identify security deficiencies in countermeasures using the MADSC methodology described in Chapter 3. The countermeasure reference tables included in Appendix B show where countermeasures have the greatest impact for facility defense. For example, installing fiber fence technology at the perimeter provides detection of an intrusion but in some cases has negligible effect on the overall degree of difficulty. Avoiding this cost in exchange for less expensive surveillance cameras with built-in analytics to detect the adversary are acceptable alternatives in many situations. Every facility is physically unique and will require explicit analysis to ensure the critical asset is protected in the best way possible. Some facilities are in a dense urban area with buildings and public streets on all sides. The exterior of the building inherits the characteristics of the perimeter, detection line, and observation zone to create a combined defense layer. Countermeasure selection in this situation will focus on what provides the best deter, detect, observe, delay, deny, and respond characteristics. Reducing the number of ingress points to the facility can reduce the total number of countermeasures required to protect the facility (Wallace et al. 2024). Additional examples of the cost–benefit analyses are discussed in Chapter 3.

2.11 RISK MANAGEMENT

Risk management (Figure 2-1) is the intentional examination of all risk components, the reduction of vulnerabilities by implementing remedial actions, or the acceptance of risk. Utility owners can make informed risk management decisions based on results from the iterative evaluation of the cumulative defense strategy process. In general, there are three options for dealing with physical security risks to a facility: mitigation, transference, or acceptance of risk.

2.11.1 Risk Mitigation Risk mitigation is the implementation of strategies to reduce or eliminate a threat or the effects of a threat. In cumulative defense strategy, the highest-level critical assets receive the greatest mitigation efforts and expense. Countermeasures and cost are minimized as the possibility of threat is further removed from the critical asset.

2.11.2 Transferring the Risk Transferring the risk can be accomplished by purchasing insurance to cover the cost of repairing or replacing the critical asset.

2.11.3 Risk Acceptance Risk acceptance is the acknowledgment that the consequence of the asset loss could cost less than the cost required to mitigate the risk. A utility may conclude that it is more cost effective to use a redundant asset or replace the asset in the event of compromise rather than implementing the recommended countermeasures. These are appropriate forms of risk acceptance because viable alternatives have been identified and approved by utility owners. Utilities that elect to compromise with risk acceptance, after performing the analysis, could be found negligent in the event of an attack if no viable alternatives were originally identified and approved by the utility owner.

This page intentionally left blank

CHAPTER 3
DETERMINING DIFFICULTY OF PHYSICAL SECURITY COUNTERMEASURES

3.1 INTRODUCTION

This chapter describes how to calculate the degree of difficulty to compromise the physical security countermeasures (hereafter called security countermeasures or countermeasures) at a water utility using the cumulative defense strategy described in Chapter 2. The degree of difficulty calculation for a given attack vector directly correlates to the probability of success of the given threat and the vulnerability of the facility to the attack.

3.2 PROBABILITY OF SUCCESS OF A GIVEN THREAT ($P_{S|T}$)

For *Defense in Depth* terms, if an adversary on foot were to choose a path of jumping over a fence to initiate an attack on a targeted asset [scenario (s_i)], with the intent of causing a catastrophic failure [consequence (c_i)], then the security countermeasures required to be defeated represents the [degree of difficulty (d_i)] to compromise the facility. If the triplets for security risk $<s_i, d_i, c_i>$ are known, then they become a function of the conditional probability of success of a given threat $P_{S|T}$ as shown in Equation (3-1).

$$P_{S|T} = f(s_i, d_i, c_i) \tag{3-1}$$

The reference tables provided in Appendix B include the information necessary to calculate the degree of difficulty to compromise the physical security countermeasures and thus the probability of success of a given threat for a scenario and consequence identified. Once this is determined, the degree of vulnerability directly corresponds to the probability of success of a given threat, $P_{S|T}$ (Wallace and Foster 2021). Section 3.6 contains an example of how to apply the reference tables to an example facility. High-level details on the Foster–Wallace formula (Wallace and Foster 2021) used to generate the data in the reference tables is documented in the following sources:

1. *A Logical Basis for Cumulative Defense Strategy and the Mathematical Analysis of Defense Strategy and Countermeasures (MADSC)* (Wallace and Foster 2021), and
2. *Empirical Risk Analysis Methodology for Adversarial Threats Against Critical Infrastructure* (Wallace et al. 2024).

3.3 MATHEMATICAL ANALYSIS OF DEFENSE STRATEGY AND COUNTERMEASURES METHODOLOGY

The Foster–Wallace formula analyzes the current defensive countermeasures mathematically and objectively to recommend optimized placements for improvements. The process of evaluation is called the MADSC methodology (Wallace et al. 2024). The MADSC methodology is used to analyze the defensive layers that encompass the entire defense strategy. Each defense layer is designed to address one or more attack vectors. Most facilities can be defended by applying four, five, or six defense layer elements to help protect the critical assets. Defense layer elements are often referred to as ordinal steps because the adversary must sequentially cross the defense layers to reach the critical asset. Path analysis for each attack vector is evaluated for the number of ordinal steps and the subset of countermeasures within each of these ordinal steps. For instance, an adversary on foot may have to breach six ordinal steps to reach a critical asset, and each step consists of multiple countermeasures that collectively bolster each ordinal step as shown in Figure 3-1. At each ordinal step, the quantity and quality of countermeasures must increase to maintain a growing minimum difficulty threshold, which in turn increases the difficulty to compromise the ordinal step. The minimum difficulty threshold concept is described in Section 3.4.

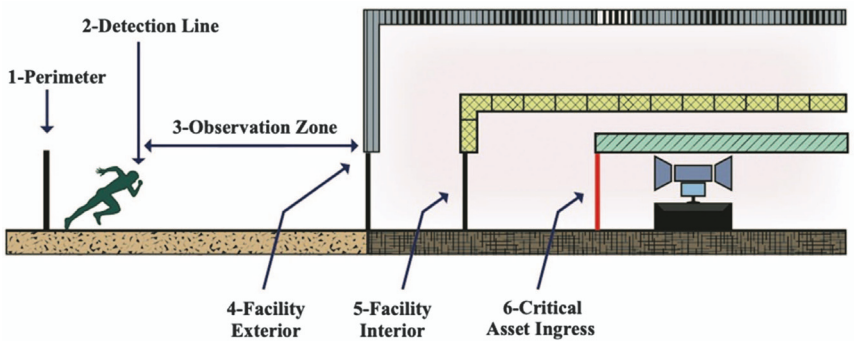


Figure 3-1. Adversary on foot attempting to cross six ordinal steps at a facility.

3.4 MINIMUM DIFFICULTY THRESHOLD

According to cumulative defense strategy, security countermeasures are required to incrementally increase in quantity and quality throughout the scale of the facility and is referred to as the MDT. The MDT establishes the minimum number of countermeasures and their characteristics required for each ordinal step. The minimum quantity of sequential countermeasures (SCM) required for each ordinal step is equivalent to the ordinal step number plus one. Countermeasure quality improvements at each ordinal step can be achieved by selecting countermeasures with increasing inherent combination of characteristics including deter, detect, observe, delay, deny, and respond as described in Section 2.7.3. This is done to force the attacker to expend more time and resources to defeat the countermeasures leading up to a full compromise.

Table 3-1 offers some guidance to appropriately select a minimum difficulty threshold based on the size and type of facility. As the population served increases, so does criticality of the water treatment facilities that serve the community. The recommendations provide options for owners and operators to consider additional physical security protection measures to help secure their facilities. Population served and available asset redundancy are important factors to consider; however, other factors not listed here should also be considered when determining a minimum difficulty threshold value.

Tables 3-2, 3-3, and 3-4 are provided to help correlate cumulative defense strategy concepts to minimum difficulty threshold requirements considering multiple facility types and sizes. For example, four ordinal steps could be appropriate to characterize a pump station in a rural setting, whereas six ordinal steps might be necessary to characterize a large water treatment plant. Considering the population served as well as facility redundancies is appropriate to associate a minimum difficulty threshold to a facility type.

Countermeasure characteristics are intrinsic to the countermeasures themselves. For example, countermeasures with respond characteristics like lights and sirens are not directly coupled with how and when to respond to an attack. Alarm systems can be triggered as soon as an intrusion is detected. Executing response procedures at the earliest point of detection is not part of the intrinsic characteristics of the countermeasures themselves (such as a flashing strobe), but it does send a response

Table 3-1. Water Facility Type and Size to Recommended MDT.

Water Facilities	Wastewater/Stormwater Facilities	Recommended MDT Ordinal Steps
WTP (population > 100k)*	WWTP/SWTP (population > 100k)	6
WTP (pop. served 50k–100k)	WWTP/SWTP (pop. served 50k–100k)	5 to 6
WTP (pop. served < 3,300)	WWTP/SWTP (pop. served < 3,300k)	4 to 6
Raw Water Facilities	Collection Systems	4 to 6
Wells and Pumping Stations	Pumping Stations	4 to 6
System Support Facilities	System Support Facilities	4 to 6
Finished Water Storage		4 to 6
Water Distribution Systems		4 to 6

*The symbol k is designated as 1,000.

Table 3-2. Four Ordinal Steps MDT.

Ordinal Steps	Defense Layer Elements	Minimum # of SCMs	Recommended Countermeasure Characteristics					
1	Perimeter	2	Deter					
2	Detection Line	3	Deter	Detect				Respond
3	Observation Zone	4	Deter	Detect	Observe	Delay		Respond
4	Critical Asset Ingress	5	Deter	Detect	Observe	Delay	Deny	Respond
	Total Countermeasures	14						

Table 3-3. Five Ordinal Steps MDT.

Ordinal Steps	Defense Layer Elements	Minimum # of SCMs	Recommended Countermeasure Characteristics					
1	Perimeter	2	Deter					
2	Detection Line	3	Deter	Detect				Respond
3	Observation Zone	4	Deter	Detect	Observe	Delay		Respond
4	Facility Exterior	5	Deter	Detect	Observe	Delay	Deny	Respond
5	Critical Asset Ingress	6	Deter	Detect	Observe	Delay	Deny	Respond
	Total Countermeasures	20						

Table 3-4. Six Ordinal Steps MDT.

Ordinal Steps	Defense Layer Elements	Minimum # of SCMs	Recommended Countermeasure Characteristics					
1	Perimeter	2	Deter					
2	Detection Line	3	Deter	Detect				Respond
3	Observation Zone	4	Deter	Detect	Observe	Delay		Respond
4	Facility Exterior	5	Deter	Detect	Observe	Delay	Deny	Respond
5	Facility Interior	6	Deter	Detect	Observe	Delay	Deny	Respond
6	Critical Asset Ingress	7	Deter	Detect	Observe	Delay	Deny	Respond
	Total Countermeasures	27						

to site personnel as an alert or notification for verification and appropriate response. Coupling the respond characteristic with detect and observe characteristics provides necessary feedback to assess the situation appropriately.

Table 3-5 represents an expanded version of Table 3-2 to show how the characteristics of countermeasures line up with the countermeasure selected in the reference tables that appear in Appendix B.

For comparison purposes, Table 3-6 reflects the expanded version of Table 3-4 to demonstrate how the countermeasure characteristics maintain effectiveness as the total number of sequential countermeasures increases. Critical thinking should be used when determining the minimum difficulty threshold required (number of defense layer elements) for the facility type under consideration. Applying a minimum difficulty threshold that is too small will result in an arbitrarily high degree of difficulty score leading to a false sense of security. The inverse is also true, resulting in an extremely low difficulty score and an overburden of countermeasures on a facility that is too small to support them.

Table 3-5. Four Ordinal Steps MDT: Countermeasure Characteristic Chart for an Adversary on Foot.

Defense Layer	SCM	Physical Security Countermeasure	Recommended Countermeasure Characteristics					
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	Deter					
	2	Posting of perimeter boundary [No Trespass signs every 50 ft (15.24 m), etc.]	Deter					
2 Detection Line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	Deter	Detect				Respond
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	Deter	Detect	Observe			Respond
3 Observation Zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	Deter			Delay		
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	8	Tracking device (Ground radar, thermal imagery, etc.)	Deter	Detect	Observe			Respond
	9	PTZ surveillance camera (Day/night coordinated with tracking device)	Deter	Detect	Observe			Respond
4 Critical Asset Ingress	10	Hardened exterior and access point(s) (Steel doors, film on glass, concrete walls, etc.)	Deter			Delay		
	11	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	Deter	Detect			Deny	Respond
	12	Unified VMS (Link sites, push scenes, send out notifications, etc.)			Observe			Respond
	13	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	14	Intrusion detection (Glass break, motion, analytic, etc.)	Deter	Detect				Respond

Table 3-6. Six Ordinal Steps MDT: Countermeasure Characteristic Chart for Adversary on Foot.

Defense Layer	SCM	Physical Security Countermeasure	Recommended Countermeasure Characteristics					
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	Deter					
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	Deter					
2 Detection Line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	Deter	Detect				Respond
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	Deter	Detect	Observe			Respond
3 Observation Zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	Deter			Delay		
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	8	Tracking device (Ground radar, thermal imagery, etc.)	Deter	Detect	Observe			Respond
	9	PTZ surveillance camera (Day/night camera coordinated with tracking device)	Deter	Detect	Observe			Respond
4 Facility Exterior	10	Emergency annunciator (PA system, 2-way audio, alarm, lighting, etc.)	Deter					Respond
	11	Intrusion detection (Glass break, motion, analytic, etc.)	Deter	Detect				Respond
	12	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	13	Hardened exterior and access point(s) (Steel doors, film on glass, concrete walls, etc.)	Deter			Delay		
	14	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	Deter	Detect			Deny	Respond
5 Facility Interior	15	Unified VMS (Link sites, push scenes, send out notifications, etc.)			Observe			Respond
	16	Hardened interior and access point(s) (Steel door, solid wall beyond drop ceiling, etc.)	Deter			Delay		
	17	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	Deter	Detect			Deny	Respond
	18	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	19	Intrusion detection (Glass break, motion sensor, etc.)	Deter	Detect				Respond
	20	Dual-factor authentication PACS secure (PACS secure + access code)	Deter	Detect			Deny	Respond
6 Critical Asset Ingress	21	Hardened interior and access point(s) (Steel door, solid wall beyond drop ceiling, etc.)	Deter			Delay		
	22	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	Deter	Detect			Deny	Respond
	23	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	Deter	Detect	Observe			Respond
	24	Intrusion detection (Camera analytic, thermal, etc.)	Deter	Detect	Observe			Respond
	25	Dual-factor authentication PACS secure (PACS secure + access code)	Deter	Detect			Deny	Respond
	26	Secondary intrusion detection (Glass break, motion sensor, etc.)	Deter	Detect				Respond
	27	Multifactor Authentication (MFA) PACS secure (PACS secure + access code + biometric)	Deter	Detect			Deny	Respond

3.5 SITE-SPECIFIC MODEL CALIBRATION

Reference tables of countermeasures calibrated for multiple facility types considering different attack vectors appear in Appendix B. The tables are intended to provide a basis for consideration, but site-specific countermeasure selection and calibration could be necessary. The following topics are appropriate to consider when selecting different countermeasures within the tables in Appendix B.

1. *Does the countermeasure meet the recommended characteristics for the ordinal step being considered based on the minimum difficulty threshold?* Keep in mind that for a given defense layer element and ordinal step, each countermeasure within the ordinal step does not need to have all the characteristics required for that ordinal step. For example, ordinal step four requires a total of five individual security countermeasures to meet the recommended minimum difficulty threshold. All five countermeasures do not need to have all six countermeasure characteristics. A surveillance camera with day/night capability and detection analytic has deter, detect, and observe characteristics, whereas an annunciator with strobe light has deter and respond characteristics. Both countermeasures combined provide four of the six recommended characteristics for that defense layer element. This provides some flexibility when selecting countermeasures for different defense layers.
2. *Is the countermeasure different from the other countermeasure within the same ordinal step?* For example, installing four identical surveillance cameras in ordinal step three, the observation zone, only counts as one countermeasure for the given path analyzed. Installing a fixed camera, thermal camera, and a PTZ camera would count as three different countermeasures because they have different capabilities and are independent from each other. Countermeasures within a defensive layer element are recommended to be unique for the methodology to work correctly and to prevent the scenario of "defeat one and compromise all."
3. *Does the countermeasure apply to defending against the attack vector under consideration?* Applying acquired sense or expert judgment is necessary to effectively select countermeasures for defense layers. Installing spiked marine bollards across a parking lot to deter vehicle traffic might be effective, but probably is not the best use of the countermeasure. Appendix A provides preliminary guidance for appropriate use of countermeasures in different environments.
4. *Does the countermeasure help address the incremental increase in quantity and quality of the overall subset of countermeasures?* Forcing the adversary to work harder and expend more resources at each step along the path makes it increasingly difficult for them to succeed. Creating a perimeter with a moat around the facility, and then installing a hollow core wooden door at the critical asset ingress, does not satisfy the recommendations.

3.6 CALCULATING DEGREE OF DIFFICULTY TO COMPROMISE COUNTERMEASURES

This section outlines the basic process of using the countermeasure reference tables found in Appendix B to mathematically determine the degree of difficulty to compromise the sum of the countermeasures based on a specific attack vector. Table 3-7 was copied from Appendix B, Table B-5, and inserted in this section for ease of reference to support the subsequent discussion. It contains the recommended countermeasures to defend a facility requiring four ordinal steps considering an AOF attack vector scenario.

Each of the physical security countermeasures in the table are discussed in Appendix A according to the associated sections referenced in the table. Designers should adhere to the manufacturer's specifications for the countermeasures discussed in Appendix A. The "Delta Difficulty" column contains the precalculated degree of difficulty to compromise value based on the Foster–Wallace formula. The values in this column are different for facilities with four, five, or six ordinal steps because the math model accounts for the changes in the minimum difficulty threshold required for more ordinal steps. The "Facility Difficulty" column is left blank and is intended to be filled out during the path analysis phase of the evaluation process.

Path analysis on the facility should be performed according to Section 2.6. During the analysis, refer to the appropriate reference table in Appendix B. At each ordinal step, consider whether the facility has the recommended countermeasures installed along the path or if there are portions of the facility where an adversary can bypass a particular set of countermeasures. Analyze all the available critical asset entry paths based on the attack vector. Enter the delta difficulty value in the "Facility Difficulty" column for each countermeasure that is present along the path to the critical asset. Each countermeasure can only be counted once per path analysis when adding the delta difficulties together for a particular attack vector. *The sum of the individual delta difficulties for each of the countermeasures represents the total degree of difficulty to compromise all the countermeasures for the analyzed path.*

The overall facility security is only as strong as the weakest path to compromise the asset. Therefore, it is critical to consider all paths leading up to the critical asset to protect the facility. When inconsistencies in the degree of difficulty to compromise values are identified, that reveals where physical security improvements can be made to help defend the facility. The process described previously is consistent for all the countermeasure reference tables included in Appendix B.

Consider an example facility with security countermeasures 1, 2, 5, 9, 10, 11, and 14 already installed from Table 3-7. For convenience, the "Facility Difficulty" column has been included to facilitate recording the delta difficulty values during the path analysis. Adding up the delta difficulty values from each of the countermeasures in the facility difficulty column results in a total degree of difficulty to compromise equal to 65.33%. It also means the facility is 34.67% vulnerable to this particular attack vector given the path analysis to the critical asset based on Section 2.8. The path for improvement now becomes clear based on the missing countermeasures from Table 3-7. Adding a tracking device, SCM 8 and coordinating it with the PTZ camera brings the degree of difficulty to compromise up to 79.35%. Also, installing the Unified VMS platform, SCM 12, in the facility brings the total difficulty up to 89.70%. Facility operators can begin to make informed decisions about the physical security of their facilities based on these results given their unique environments.

3.7 EXPANDED COST–BENEFIT ANALYSIS DISCUSSION

Continuing with the previous example, improvements to physical security can be considered from a cost–benefit perspective as well using Table 3-7. Considering that SCMs 1, 2, 5, 9, 10, 11, and 14 are already installed, the cost of the individual missing countermeasures can be determined through standard bidding processes. The contribution of each independent countermeasure is already known because of the delta difficulty value presented in the table. Comparing the cost of installation versus the added delta difficulty value reveals how facility operators can improve their physical security in a cost-effective way.

Table 3-7. Countermeasure Reference Chart, Four Ordinal Steps: Adversary on Foot.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	7.05×10^{-18} small number	*7.05×10^{-18}*
	2	Posting of perimeter boundary [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	5.76×10^{-10} small number	*5.76×10^{-10}*
2 Detection Line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	2.10×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	*0.1516*
3 Observation Zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	6.0	0.7349	
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	9.0	4.8853	
	8	Tracking device (Ground radar, thermal imagery, etc.)	7.0	14.0142	
	9	PTZ surveillance camera (Day/night coordinated with tracking device)	9.0	23.1013	*23.1013*
4 Critical Asset Ingress	10	Hardened exterior and access point(s) (Steel doors, film on glass, concrete walls, etc.)	10.0	21.6223	*21.6223*
	11	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	8.0	19.1052	*19.1052*
	12	Unified VMS (Link sites, push scenes, send out notifications, etc.)	9.0	10.3558	
	13	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	4.2298	
	14	Intrusion detection (Glass break, motion, analytic, etc.)	7.0	1.3534	*1.3534*
			Sum of Facility Difficulty values		***65.33***

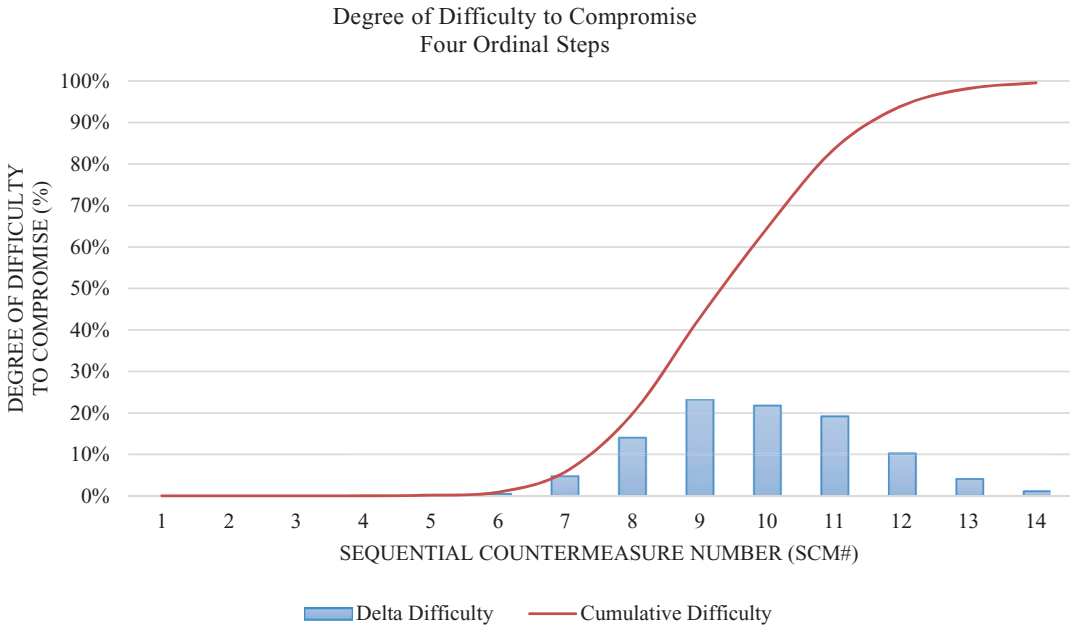


Figure 3-2. Degree of difficulty to compromise countermeasures curve: four ordinal steps.

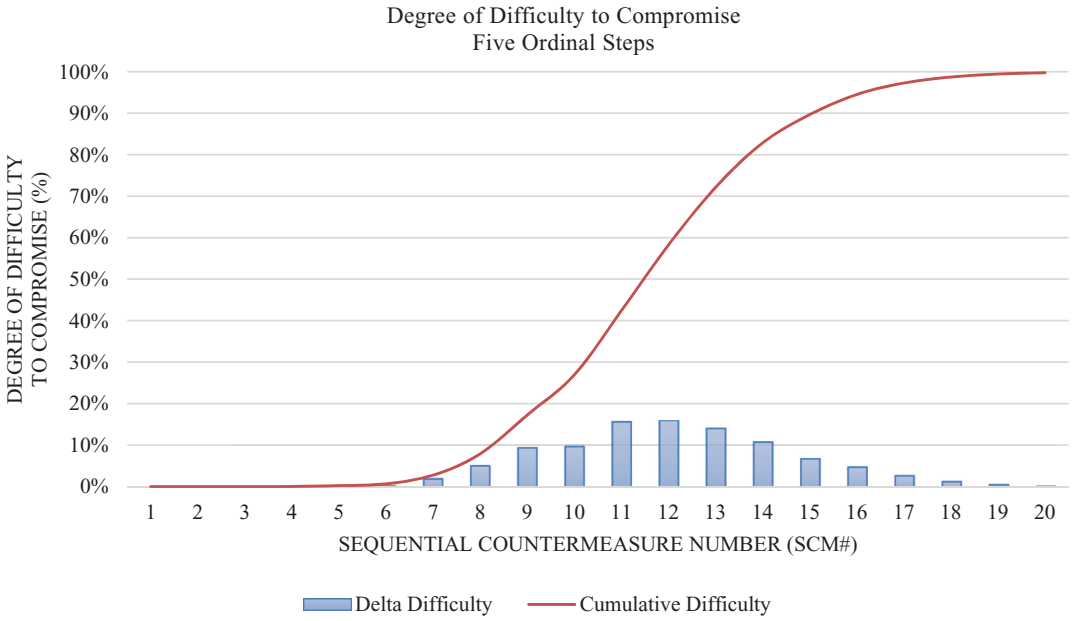


Figure 3-3. Degree of difficulty to compromise countermeasures curve: five ordinal steps.

The same approach works for comparing the cost of two different types of countermeasures for the same sequential countermeasure number. For example, SCM 8 recommends a sensor with tracking capability. Ground radar and thermal sensors are two great options, depending on the installation environment and their capabilities. In some cases, the individual cost of the countermeasures might be similar, but when the total installation cost is considered, one might be considerably better from a financial perspective.

It is important to note the shape of the cumulative difficulty curve for a four-ordinal-step defense strategy in Figure 3-2. Perimeter fences and signs, SCMs 1 and 2, often have a low degree of difficulty to compromise but are necessary to establish a legal demarcation for prosecution purposes. The detection line, SCMs 3, 4, and 5, also do not exhibit any real stopping power against an attack but are necessary to provide advanced warning to begin executing response procedures. The observation zone, SCMs 6, 7, 8, and 9, reflect the importance of maintaining awareness of the target and assessing the situation to have the best information moving forward. The critical asset ingress, SCMs 10, 11, 12, 13, and 14, establish the hardened defense of the asset with strong delay and deny countermeasure characteristics. Understanding where countermeasures have the greatest impact for defending the asset can be used to justify the cost associated with the protection measure. Cumulative difficulty curves for five and six ordinal steps are shown in Figures 3-3 and 3-4, respectively.

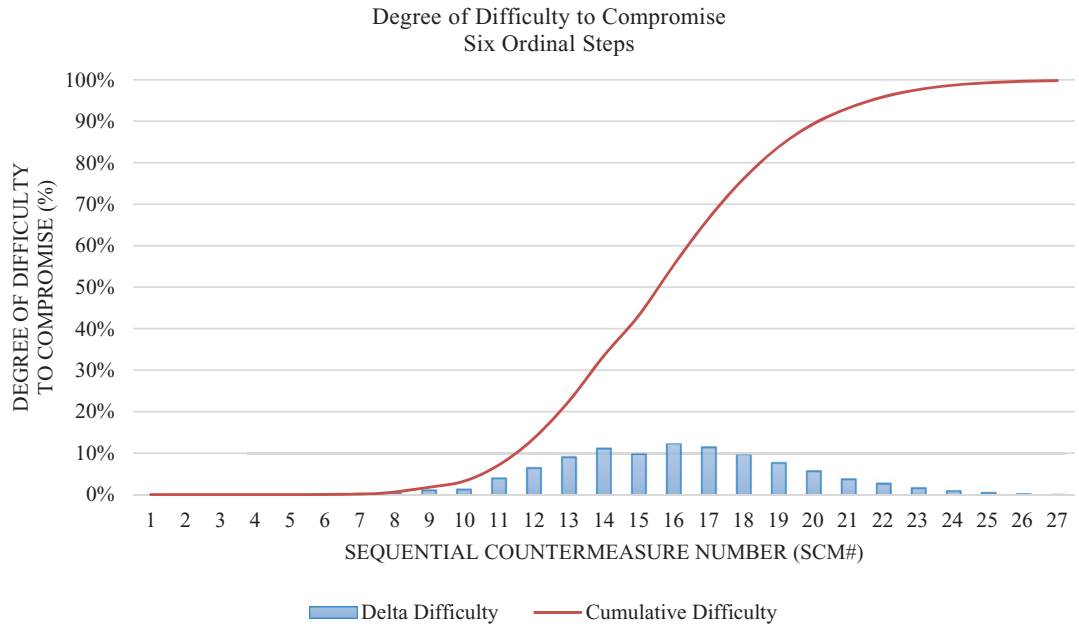


Figure 3-4. Degree of difficulty to compromise countermeasures curve: six ordinal steps.

This page intentionally left blank

APPENDIX A
PHYSICAL SECURITY COUNTERMEASURES

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 water and/or wastewater/stormwater utility. For critical assets that are not owned by the water and/or wastewater/stormwater utility, protection of the assets needs to be coordinated with their owners.

A.1 FENCING AND PERIMETER WALLS

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

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

A.1.1 Chain-Link Fencing For terms related to chain-link fencing systems, refer to ASTM F552-14, *Standard Terminology Relating to Chain Link Fencing* (ASTM 2019). For detailed specifications and design information related to chain-link fencing and posts, refer to US DOD UFC 4-022-03, *Security Fences and Gates* (US DOD 2013). This document has been approved for public release and is available online. Aluminum fabric, poles, or accessories are not recommended for security applications.

Where fences cross a stream, culvert, swale, depression, or other openings that fencing does not enclose, where the opening size is 96 in.^{2} (62,000 mm^2) or larger, these openings should be protected by additional grilles, fencing, or other barriers against penetration. Refer to Section A10.2.2 and to US DOD UFC 4-022-03, *Security Fences and Gates* (US DOD 2013), for recommendations and construction of grilles.

A.1.2 Anti-Climb/Anti-Cut Fencing A specialized anti-climb/anti-cut fence such as wire-panel mesh fencing should be considered. For detailed specifications and design information related to anti-climb/anti-cut fencing, refer to US DOD UFC 4-022-03, *Security Fences and Gates* (US DOD 2013). This document has been approved for public release and is available online.

A.1.3 Ornamental Fencing Site conditions and local codes may dictate the use of aesthetically pleasing fence materials. In such cases, ornamental fences of steel, aluminum, or wrought iron should be considered. For detailed specifications and design information related to ornamental fencing, refer to US DOD UFC 4-022-03, *Security Fences and Gates* (US DOD 2013). This document has been approved for public release and is available online.

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

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

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

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

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

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

A.1.5 Fence Topping Fence topping may include barbed-wire topping or concertina barbed-wire tape topping, or a combination of both. Ornamental fencing with angled "pikes" can be provided as a fence topping to discourage or prevent access to a facility by climbing. For detailed specifications and design information related to fence topping or top guards, refer to US DOD UFC (UFC 4-022-03), *Security Fences and Gates* (US DOD 2013). This document has been approved for public release and is available online.

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

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

A.1.7 Fence Foundation Enhancements To prevent stretching of the fence fabric to allow an adversary to move under the fence, it may be appropriate to anchor the bottom fabric of the fence to create a delay like that for solid fencing. For anchorage of fabric, the bottom of the fence fabric should be secured to a bottom rail and securely anchored at the midpoint between the fence posts along the fence line. The bottom rail may be anchored to an eyebolt embedded in a deadman anchor. The deadman should be buried in the soil below the fence rail. For detailed specifications and design information related to fence foundation enhancements, refer to US DOD UFC 4-022-03, *Security Fences and Gates* (US DOD 2013). This document has been approved for public release and is available online.

A.2 GATES

Personnel gates should follow similar construction guidelines as fences, or stronger, whereas vehicle gates need additional

strength due to the weight of the gate assembly as well as to prevent vehicle incursion.

A.2.1 Chain-Link Gates For detailed specifications on chain-link gates, refer to US DOD UFC 4-022-03, *Security Fences and Gates* (US DOD 2013). This document has been approved for public release and is available online.

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

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

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

Electric motors should be sized appropriately for the gate size, duty rating, and frequency of operation. Provide industrial-quality motor overload protection with manual reset. Gate operators and other electrical appurtenances should be positioned within the fenced perimeter to avoid vandalism and tampering.

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

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

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

Component parts of the gate operator, including attachments, should be constructed with materials, or plated, coated, or finished as necessary to provide reliable service in an all-weather environment. For detailed specifications on gate automation, refer to US DOD UFC 4-022-01, *Entry Control Facilities Access Control Points* (US DOD 2017). This document has been approved for public release and is available online.

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

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

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

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

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

A.2.4 K-rated Gates K-rated gates are designed to withstand an impact from a vehicle within the parameters of a defined maximum mass and speed. Higher k-ratings directly correspond to withstanding impacts of heavier vehicle traveling at greater speeds. For detailed specifications on K-rated gates, refer to US DOD UFC 4-022-02, *Selection and Application of Vehicle Barriers* (US DOD 2010b). This document has been approved for public release and is available online.

A.3 SIGNAGE

A.3.1 Fence Signage Post "No Trespassing" signs at 50 ft (15 m) intervals in multiple languages as is consistent with the local population. From a general legal standpoint, the fence and signage establish a boundary that intruders must cross for violation.

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

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

A.3.2 Primary Site Entrance Signage At the primary entrance to the site, post the address of the site so that first responder crews (such as police and fire departments) can confirm the address location.

A.3.3 Water Intake Delineation At lake or river intakes, provide buoys or float lines with appropriate signage to delineate no-entry zones.

A.4 OUTDOOR SECURITY LIGHTING

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

In addition to the suggested illumination levels provided subsequently, refer to *Guideline for Security Lighting for People, Property, and Public Spaces* (G-1-03) (IESNA 2016).

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

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

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

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

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

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

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

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

When surveillance cameras are used, these additional lighting considerations should be taken ("Protection of Assets Physical Security," Chapter 6: Lighting) (ASIS 2012):

- Color-rendering index: Choose an appropriate lamp that has accurate color reproduction.
- Reflectance of materials: Consider the material that will be illuminated and its ability to reflect and transmit light.
- Direction of reflected lighting: Identify whether reflected lighting will assist or interfere with camera operation.

A.5 BOLLARDS AND OTHER VEHICLE BARRIERS

Vehicle barriers can take on many shapes and forms. They can include things such as ditches, berms, fencing, jersey barriers, trees, boulders, and the like. Not all barriers are designed to be impact rated. Depending on the level of hardening desired according to the countermeasure reference tables, care must be taken to ensure that the barrier is impact rated according to design specifications.

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

Refer to US DOD UFC 4-022-02, *Selection and Application of Vehicle Barriers* (US DOD 2010b), for detailed descriptions, attributes, and stopping capabilities of several barrier types. Refer to US DOD UFC 4-022-01, *Entry Control Facilities Access Control Points* (US DOD 2017), for detailed descriptions of access control entry points. Both documents have been approved for public release and are available online and should be referenced for all the subpoints in Section A.5.

A.5.1 Speed Reduction Techniques Vehicle speed reduction techniques are important to consider when designing and developing vehicle entry paths. The total kinetic energy a moving vehicle can develop is directly proportional to the mass of the vehicle multiplied by its velocity squared. The mass of the vehicle is a constant, but the speed squared term begins to grow rapidly as the vehicle moves faster. Using techniques to reduce the maximum achievable vehicle speed can be accomplished by implementing some of the following items along the vehicle entry path to the facility. This list is not comprehensive, and other vehicle speed reduction techniques could be used instead of those listed next.

A.5.1.1 Reverse Pitch Corner Reverse pitch corners back-to-back create an "S" pattern in the road requiring vehicles to use slower speeds to navigate the turn without going off the road.

A.5.1.2 Tight-Angled Entry Tight entry angles off main roads or on the property forces vehicles to use slower speeds to maintain control of the vehicle to make the turn.

A.5.1.3 Staggered Barriers Staggered barriers require vehicles to use slower speeds to navigate through them.

A.5.1.4 Approach Straightaway Distance Limiting the approach straightaway distance can help reduce the maximum achievable speed that a vehicle could reach before breaching a critical asset. For example, locating a main entry gate, or a critical asset building at the end of a long straightaway in a road is not recommended.

A.5.2 Entry and Exit Vehicle Flow Control Maintaining control over the flow of vehicle traffic in and out of a facility is important to overall defense strategy. Installing security measures to facilitate this process can help defend a facility against malevolent attacks.

A.5.2.1 Sallyport A sallyport is a combination of electrically operated gates or portals that are interlocked to prevent more than one gate from opening at a time. The sallyport provides a means for secured, controlled entry through the fence perimeter of the facility. Entry processing, paperwork review, and driver/load identification or verification occur within the sallyport. Sallyports may also be used to enable searching the interior and undercarriage of vehicles for explosives.

Typical vehicle sallyport dimensions are in the range of 75 ft (23 m) long by 20 ft (6 m) wide and should be sized to accommodate the largest delivery vehicle. The sallyport should be enclosed by fenced sides of height, construction, and configuration consistent with the site perimeter fencing. Vehicle gates should be consistent with the gate guidelines provided in Section A.2.

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

Gate controls should be located such that the person operating the controls maintains a constant visual observation of the sallyport area. The controls should be protected and covered so that unauthorized use is eliminated.

A.5.2.2 Barriers Separating Entry and Exit Driveways Separating entry and exit driveway paths enables the use of different types of physical security countermeasures for inbound and outbound traffic. The entry path could utilize a sallyport while the exit path could incorporate reverse tire puncture strips.

A.5.2.3 Single Entry and Exit Points to Facility Parking Areas Creating a choke point with one entry point and one exit point to the facility parking area allows surveillance to be focus on one critical location.

A.5.3 Full Perimeter Vehicle Barrier A full perimeter vehicle ramming breach barrier can include the application of multiple types of barriers to prevent vehicles from breaching any location around the perimeter. Leveraging natural terrain such as rivers, trenches, ditches, and densely wooded areas can create effect barriers to a vehicle breach. Physically constructed countermeasures including bollards, Jersey barriers, and guardrails can also be implemented to support the desired level of protection.

A.5.4 Facility Barrier Protection

A.5.4.1 Parking Lot Standoff Distance Refer to US DOD UFC 4-010-01, *Minimum Antiterrorism Standards for Buildings* (US DOD 2022) for detailed descriptions about standoff distances for facilities.

A.5.4.2 Barrier between Parking Areas and the Facility K-rated bollards and barriers should be placed between the parking area and the facility to help defend against vehicle ramming breach scenarios.

A.6 OPEN SPACE (OBSERVATION ZONE)

A.6.1 Open Space between Detection Line and the Facility Visually unobstructed space should be present from all facility approach angles between the detection line and the facility exterior. Areas should be clear of landscaping and structures that could interfere with detection and observation countermeasures.

A.7 ELECTRONIC SECURITY SYSTEMS

A.7.1 Intrusion Detection Sensors: General The intrusion detection system should be capable of detecting an individual [weighing 75 lb (34 kg) or more] crossing the detection zone walking, crawling, jumping, running, or rolling [at speeds between 0.5 and 15 ft/s (0.2 and 4.6 m/s)], or climbing the fence, if applicable.

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

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

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

Intrusion detection systems should cover all vehicle and pedestrian access points through the perimeter. In some scenarios, it might not be economically feasible to install intrusion detection systems along the entire perimeter because the fences could extend for miles. Using countermeasures like ground radar systems in conjunction with PTZ cameras located near the facility may move the detection line inside the perimeter fence but could be more cost effective than installing detection systems at the perimeter.

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

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

A.7.2 Exterior Intrusion Detection Prevalent sensor technologies include active infrared, microwave, dual-technology, buried line, fence-mounted sensors, video motion detection, and ground radar.

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

A.7.2.1 Active Infrared Sensors Active infrared sensors transmit infrared signals to a receiver. Interruption of the signal indicates that an intruder or object has blocked the path.

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

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

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

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

A.7.2.2 Microwave Sensors Microwave sensors transmit or flood a designated area with an electronic field. A movement in the area disturbs the field and sets off an alarm.

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

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

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

A.7.2.3 Dual-Technology Sensors Dual-technology sensors use both microwave and PIR sensor circuitry within the same housing. PIR sensors pick up heat signatures from intruders by comparing infrared receptions to typical background infrared levels. Typically, activation differentials are 3 °F (1.7 °C).

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

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

Nuisance alarms for microwave sensors are described in Section A.7.2.2. Nuisance alarms for PIR sensors include reflected light and radiated heat.

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

A.7.2.4 Buried Line Sensors There are several types of buried line sensors, including fiberoptic cable, ported cable, and ported coaxial cable.

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

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

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

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

A.7.2.5 Fence-Mounted Sensors Fence-mounted sensors detect vibrations on fence fabric associated with sawing, cutting, climbing, or lifting the fence fabric.

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

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

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

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

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

A.7.2.6 Thermal Cameras Thermal cameras detect infrared radiation emitted from objects and create images based on the sensed information. Thermal images provide good information when there are significant temperature differences between the object of interest and the background scene. They can be used for object detection in multiple weather conditions and total darkness. Supplemental illumination is not necessary for thermal cameras to function properly. Thermal cameras cannot be used for identifying characteristics about an individual or make and model of a vehicle like an optical surveillance camera equipped with software analytics (Nilsson and AXIS Communication 2017).

A.7.2.7 Ground Radar Ground radar systems are capable of detecting and tracking multiple targets at the same time. Built-in advanced analytics can detect and track humans, vehicles, and watercraft, with a low false alarm rate. Detection area coverage is typically dependent on the radar technology used by the manufacturer. Some systems use a rotating array to provide full 360 degree coverage, whereas other solid-state devices have no moving parts and require multiple units back-to-back to provide the same coverage. Detection distance ranges from a couple hundred feet to multiple miles. Many ground radar systems are designed to integrate with existing physical security software platforms and can be coordinated with PTZ cameras to visually track targets as well. Additional software analytics can also include speed and direction monitoring (Teledyne FLIR 2021).

An emerging threat to critical infrastructure is from UAS, more commonly known as drones. These novel aircraft systems are not easily detected by traditionally deployed sensors. The small size, fast speed, and nimble maneuverability that these aircraft possess also makes them very difficult to detect. One effective method to detect and track drones is to use a radar system. A radar system must be able search a large volume of airspace to create a wide surveillance area in three dimensions, and it must have the sensitivity to track small objects and the data fidelity to identify drones (Echodyne 2019).

A.7.3 Interior Intrusion Detection Provide appropriate interior intrusion detection for the building environment.

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

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

A.7.3.1 Dual-Technology Motion Sensors Dual-technology motion sensors use passive infrared and microwave technology to detect motion. Described in Section A.7.2.3, these sensors are applicable for both interior and exterior applications.

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

Nuisance alarms can be generated from heat-radiating objects such as heat system registers or other warm objects.

A.7.3.2 Linear Beam Sensors Linear beam sensors transmit a beam of infrared light to a remote receiver, creating an "electronic" fence. Once the beam is broken, an alarm signal is generated. It has a high probability of detection and a low false alarm rate.

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

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

Nuisance alarms can be created by any objects that may break the beam, such as blowing trash or animals.

A.7.3.3 Glass-Break Sensors There are three basic types of glass-break sensors: acoustic sensors (listen for an acoustic sound wave that matches the frequency of broken glass), shock sensors (feel the shock wave when glass is broken), and dual-technology sensors (sense acoustic and shock vibrations).

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

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

A.7.4 Door and Hatch Contact Alarm Switches Door and hatch contact alarm switches should interface with a security monitoring system in addition to the SCADA system.

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

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

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

A.7.5 Pipeline Vibration Detection Technologies are being developed that provide vibration detection within pipeline sections. Incorporating this technology can detect attempts at sabotage such as cutting, hammering, or detonation of the pipeline,

and a response can be initiated. Such detection systems might be considered for critical pipeline sections that do not have redundancy. The detection systems monitor vibration within the pipeline section. If the vibration level exceeds a threshold amount, then an alarm could be transmitted back to a central monitoring station. Such systems are relatively new technology but are currently in operation for critical utility (oil, natural gas) pipelines within the United States.

A.8 PHYSICAL ACCESS CONTROL SYSTEMS

A.8.1 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: industrial grade key locks, electronic or key padlocks with shields, numeric keypad locks, or card reader systems with secure encryption technology.

A.8.2 Locks and Padlocks Padlocks should be weather-resistant with a hardened-steel shackle. The shackle should incorporate reduced access or hidden access within the locking mechanism.

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

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

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

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

Industrial grade key locks should use hardened-steel inserts protecting the plug face, shell, and sidebar from drilling attack. Shields should also be incorporated to increase the difficulty to compromise.

A.8.3 Numeric Keypad Locks Numeric keypad locks are locking systems that include a programmable keypad in addition to the door latch or deadbolt and lever handle. A user must enter a code at a keypad before the door unlocks and allows access. New codes can be added or changed at the keypad.

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

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

A.8.4 Card Reader Systems Card reader systems should incorporate the following:

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

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

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

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

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

Refer to NFPA 101, *Life Safety Code* (NFPA 2018) for code guidance on egress and ingress doors.

A.8.5 Dual-Factor Authentication Dual-factor authentication requires a minimum of two authentication identifiers to gain access to a particular area. Authentication identifiers can include the following:

1. Coded: The user knows a password, personal identification number (PIN), or phrase.
2. Credential: The user has a physical access control system (PACS) card, security token, cell phone, or security application.
3. Biometric: The user is physically identified by a fingerprint, facial recognition, retinal scan, or voice recognition.
4. Location: The user is in the proper location while attempting to gain access based on Global Positioning System (GPS) data from a cell phone or the like.
5. Time: The user is attempting to gain access within a specific time and is denied access outside the time window.

For additional information on PACS systems, refer to US DOD UFC 4-021-02, *Electronic Security Systems* (US DOD 2019).

A.8.6 Multifactor Authentication Multifactor authentication requires a minimum of three authentication identifiers to gain access to a particular area. The phrases "what you know," "what you have," and "who you are" combines the first three authentication factors from the preceding list to gain access to a restricted area.

A.9 SURVEILLANCE CAMERAS

A.9.1 General Considerations Surveillance cameras, also known as CCTV cameras, can be analog or IP network cameras, depending on factors such as suitability of the installation, site conditions, and availability of local area networks.

Multiple surveillance camera types including fixed position, pan tilt zoom (PTZ), multi-sensor, and thermal cameras are all capable of detecting intrusion scenarios or monitoring assets with advanced analytics.

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

A.9.2 Field of View Provide fixed-position or PTZ cameras depending on the desired field of view and the intended application.

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

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

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

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

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

A.9.3 Housing and Mounts Surveillance camera housing should be adequate for the intended application and site location.

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

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

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

A.9.4 Video Network Servers The video network server should be a high-performance IP network-compatible video system.

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

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

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

A.9.5 Digital Video Recorders Adequate digital recording capacity for all cameras should meet facility IT standards. No less than 30 days of continuous storage is recommended.

Consideration should be given to failover redundancy systems and long-term video archiving.

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

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

A.9.6 Unified Video Management System Consideration should be given to unified video management systems that allow mutual access to a single database for video management, intrusion detection, and access control systems from within the same software platform.

A.9.7 Video Analytics Numerous video analytics have been developed for surveillance cameras to facilitate detection in the following areas:

1. Analytics for security: Some examples of analytics for security include video motion detection, camera tampering detection, object tracking, and fire/smoke detection.
2. Analytics for business: Some examples of analytics for business intelligence and operations include object classification, object counting, people counting, dwell time and heat mapping, and traffic management.
3. Analytics for hybrid operations: Some examples of analytics for hybrid operations include automated object tracking, license plate recognition, and facial recognition capability.

For additional information on video analytics, refer to *Intelligent Network Video: Understanding Modern Video Surveillance Systems* (Nilsson and AXIS Communication 2017).

A.9.8 Restricted Surveillance Equipment Vendors The United States passed the John S. McCain National Defense Authorization Act (NDAA) designed to restrict the use, procurement, or sale of specific brands of surveillance equipment for federal agencies according to Section 889 (US Congress 2018). While this is a requirement for federal agencies, it is recommended that privately or publicly held water utilities consider this as well. Back door infiltration through intentionally compromised surveillance equipment can lead to unexpected vulnerabilities throughout the facility. Some of the currently prohibited security equipment suppliers include the following:

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

A.10 FACILITY HARDENING

A.10.1 General When new buildings are being designed, discuss with the building architect and structural engineers the opportunity to incorporate design elements that prevent progressive collapse of the facility in the event of explosion within or adjacent to the building. Progressive collapse is defined by ASCE/SEI in *Minimum Design Loads for Buildings and Other Structures* (ASCE 2022) 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." For detailed specifications on protecting facilities against detonation pressure waves, refer to *Blast Protection of Buildings*, ASCE/SEI 59-11 (ASCE 2011).

A.10.2 Exterior Hardening Exterior access points should use similar alarm contact hardware, such as magnetic door contact switches, depending on the final design. Interconnect the alarm contacts to a security monitoring system.

A.10.2.1 Doors Exterior doors should be heavy-duty, steel-metal doors conforming to ASTM F476-14, *Standard Test Methods for Security of Swinging Door Assemblies* (ASTM 2014), prepped for security door hardware. Doors should comply with ANSI/NAAMM/HMMA 862-13 *Guide Specifications for Commercial Security Hollow Metal Doors and Frames* (ANSI/NAAMM/HMMA 2013).

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

The door frame should be heavy duty with concrete fill.

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

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

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

- Glazed exterior doors and frames should be steel and meet the requirements of SDI Grade III with a G-90 galvanic zinc coating. Glazing should have appropriate protection such as security film or wire mesh installed to help prevent intrusion.

- Hinges, hinge pins, and hasps must be secured against unauthorized removal by using spot welds or pined mounting bolts.
- All exterior doors must have automatic closers.
- The exterior side of the door should have a lock guard or astragal to prevent jimmying of the latch hardware.
- Doors used for egress only should not have any operable exterior hardware.

A.10.2.2 Security Grilles Security grilles (for windows, louver openings, roof hatches, culverts, etc.) should be woven No. 10 wire gauge steel, 1.5 in. (38 mm) diamond mesh, or welded No. 10 wire gauge, 2 in. (50 mm) square welded mesh screens.

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

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

For enhanced-level threat protection, refer to US DOD UFC 4-022-03, *Security Fences and Gates* (US DOD 2013), for security grilles.

A.10.2.3 Security Cages Caged partitions (for critical equipment, pumps, motor control centers, and so on) should be No. 10 wire gauge steel with 2 in. (50 mm) welded openings in 1.25 × 1.25 × 0.125 in. (32 × 32 × 3 mm) angle iron framework.

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

A.10.2.4 Valve Operators Provide locking covers for valve operators and exterior chemical line connections.

A.10.2.5 Roof or Sidewalk Hatches Provide a lock on a manufacturer's metal door system that is set into a concrete curb with a gutter and drain.

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

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

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

A.10.2.6 Roof Vents Provide metal roof vents with numerous small openings rather than vents with fewer, larger openings [96 in.^{2} (62,000 mm^2) is considered a person-passable opening]. Contaminants can be introduced through much smaller vents; prevent direct passage of contaminants through a vent by using traps.

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

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

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

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

A.10.2.7 Vault Hatch with Elevated Curb Provide a lock on a manufacturer's door system. Alarm the vault hatch using exterior-rated magnetic door contacts.

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

A.10.2.8 Vault Door Hatch Set Flush with Top of a Structural Slab Provide a lock on a manufacturer's door system. Alarm the vault hatch using exterior-rated magnetic door contacts.

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

A.10.2.9 Blast Rated Exterior Refer to ASCE/SEI 59-11, *Blast Protection of Buildings* (ASCE 2011), for full building exterior blast rating design and construction.

A.10.3 Interior Hardening Facility interior access points and walls should be physically hardened with increasing levels of difficulty to compromise as the critical asset is approached.

A.10.3.1 Doors Interior doors should be heavy-duty, steel-metal doors conforming to ASTM F476-14 Grade 40 high-security-level door (ASTM 2014), prepped for security door hardware. Doors should comply with ANSI/NAAMM/HMMA 862-13, *Guide Specifications for Commercial Security Hollow Metal Doors and Frames* (ANSI/NAAMM/HMMA 2013).

Doors should have a maximum window opening of 96 in.^{2} (62,000 mm^2) or nominal 4 × 16 in. (100 × 400 mm) size with a minimum side panel size. Glass should have security mesh installed inside.

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

Consider electronic door status monitoring for door-forced and door-ajar conditions. This condition is satisfied if a PACS secure access control system is installed.

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

- Hinges, hinge pins, and hasps must be secured against unauthorized removal by using spot welds or pined mounting bolts.
- All interior doors must have automatic closers.

A.10.3.2 Walls Interior walls between areas of increasing security should be hardened by extending the existing walls from the floor slab (true floor) to the underside of the roof deck (true ceiling). This includes ensuring that walls extend beyond any drop ceilings to the true ceiling above. Rooms with raised floors should also be secured with walls that extend to the true floor surrounding the room. Ducting between rooms of increasing security should be fitted with grills according to Section A.10.2.2.

A.10.3.3 Windows Interior windows between areas of increasing security should be hardened by including security mesh within the window or applying a security film to the window.

A.10.3.4 HVAC Ducts Heating ventilation and air conditioning (HVAC) ducts between rooms of increasing security should be protected with grills as described in Section A.10.2.2.

A.11 INTRUSION NOTIFICATION SYSTEMS

A.11.1 Mass Notification Systems Mass notification systems can be used to communicate with personnel on site to alert them of potential danger and provide instructions to follow for their safety. These systems can also be used to address the adversary directly to potentially deter the attack. For detailed specifications and design information related to mass notification systems, refer to US DOD UFC 4-021-01, *Design and O&M: Mass Notification Systems* (US DOD 2010a). This document has been approved for public release and is available online.

A.11.2 Alarms, Sirens, Signal Lighting, and Strobes Alarms, sirens, signal lighting, and strobes can be integrated into security systems to provide audio and visual alert mechanisms in response to an intrusion. These systems serve to alert on-site personnel of an unfolding situation and inform the attacker that they have been detected. This may be enough to deter the attacker from further progress.

A.12 TACTICAL DETERRENCE

A.12.1 Human Capital Guards or security forces are recommended for facilities where the loss of life is possible due to a malevolent attack. Facilities such as dams and treatment plants serving large populations should consider the use of human capital to help protect their facility.

A.12.2 Trained Animals Trained animals such as guard dogs can be effectively used to complement the use of human capital for asset protection. Patrols can be established to watch over large areas or support dedicated access points to detect harmful substances entering the property or deter potential attackers.

A.12.3 Long-Range Acoustic Device Long Range Acoustic Device (LRAD) systems provide the ability to send warnings and notifications by communicating clearly out to 16,404 ft (5,000 m) with sound pressure levels capable of rising above surrounding noise levels. This type of device can be used to establish large safety zones with audio communication to help prevent misunderstandings (Genasys 2022).

A.12.4 Targeted Illumination Long-range, high-intensity, targeted and tracking illumination can be used for lighting up adversaries and tracking them when coordinated with tracking sensors.

A.13 SECURITY, CONTROLS, AND SCADA WIRING

All security, controls, and SCADA wiring should be protected within conduit. Security wiring should be electrically separated from SCADA and controls wiring. IP-based security cameras and sensors should have their own independent network apart from all facility control systems. This separation is important to prevent compromising one aspect and defeating both security and SCADA control systems. In other words, security countermeasures and IP surveillance cameras should not be connected or routed on SCADA/PLC networks.

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

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

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

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

Refer to NFPA 70, *National Electrical Code* (NFPA 2017), for code guidance on electrical wiring requirements.

A.13.1 SCADA and Electrical Control Panel Enclosures Provide a tamper switch at all security and SCADA control panel enclosures. Upon enclosure door opening, an alarm condition should be logged by the security monitoring system.

A.13.2 IT Equipment Enclosures Provide a tamper switch at all IT cabinets that contain sensitive equipment required for proper operation, communication, and security of the facility. Upon enclosure door opening, an alarm condition should be logged by the security monitoring system.

A.14 ONLINE WATER QUALITY MONITORING

A suite of online instruments to monitor certain surrogate water quality parameters should be installed (Kroll 2006). Among the parameters to monitor in water distribution systems are pH, chlorine residue (either total or free, depending on the type of residue maintained in the system), specific conductance, turbidity, and total organic carbon. Other indicators to consider include pressure change abnormalities, unusual temperature, dissolved oxygen, and oxidation–reduction potential.

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

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

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

Recognizing that surrogate parameter changes may be difficult to interpret from a security perspective, the utility should review and consider any physical security monitoring anomalies, such as intrusion alarms, surveillance camera records, and customer complaints related to system operations in its evaluation. For drinking water, customer complaints related to changes in color, odor, or taste should be investigated.

A.15 CHEMICAL FILL-LINE LOCKING DEVICES

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

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

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

A.16 HYDRANTS

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

Provide a one-way check valve minimizing the possibility of accidental or intentional contamination of drinking water via the hydrant. The device should not hinder or slow response time to firefighters or reduce flow below the flows referred to by ANSI/AWWA C502-18 and ANSI/AWWA C503-18 (ANSI/AWWA 2018a, b). The check valve must be capable of being tested without being removed from the hydrant to ensure a leak-proof seal.

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

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

A.17 MANHOLES

Securing manholes can be accomplished in multiple ways by including the following:

1. Tack welding provides a fast method of securing manholes. It is economical and effective for manholes not frequently accessed. The disadvantage is that the tack weld must be removed or broken before utility staff can access the manhole.
2. Bolt locks anchor the manhole to the manhole frame. They have a specialized bolt head that requires a specialized tool to unbolt or unlock the manhole. To remove or access the manhole, the bolt locks must be removed. This system of locking manholes is more flexible than the tack welding method, but more expensive to install. There are some challenges with noise and rattling on locking manhole covers.
3. Pan locks prevent entry into the manhole, as well as eliminating dumping into the collection system. The pan unit is installed into the manhole, with the edge of the pan resting within the manhole opening. The manhole is then locked in place in the pan unit. This system of locking manholes is more flexible than the tack welding and bolt locking methods, but more expensive to install.

A.18 SITE UTILITIES

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

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

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

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

Electrical lines should be placed underground where applicable.

APPENDIX B
PHYSICAL SECURITY COUNTERMEASURE REFERENCE TABLES WITH TYPICAL APPLICATION DRAWINGS

B.1 INTRODUCTION

The physical security countermeasures reference tables are created to help guide facility owners, operators, and assessors with a repeatable and unbiased methodology based on the Foster–Wallace Formula (Wallace and Foster 2021) to mathematically calculate the degree of difficulty to compromise countermeasures. The Foster–Wallace Formula relies on cumulative defense strategy to establish an appropriate MDT for each facility under evaluation. Table B-1 provides general MDT recommendations for each facility type.

The minimum difficulty threshold establishes the minimum number of countermeasures and the countermeasure characteristics required for each ordinal step. The minimum number of SCMs required for the ordinal step is the ordinal step number plus one. This satisfies the increasing countermeasure quantity requirement recommended by the cumulative defense strategy. The increasing countermeasure quality requirement is achieved by making sure that the countermeasures selected for the ordinal steps contain an increasing number of countermeasure characteristics including deter, detect, observe, delay, deny, and respond as described in Section 2.7.3. The countermeasure reference tables included in this appendix contain countermeasure recommendations that satisfy the MDT requirements for the Foster–Wallace Formula. The delta difficulty values in the reference tables have been precalculated using the Foster–Wallace Formula to alleviate the heavy burden of purchasing an advanced mathematics software to solve the formula independently.

B.2 COUNTERMEASURE REFERENCE TABLE MATRIX

The countermeasure reference table matrix in Table B-2 provides a convenient way to select the appropriate table recommended for the MADSC methodology analysis (Wallace et al. 2024) based on the facility type and attack vector.

B.3 COUNTERMEASURE REFERENCE TABLES OVERVIEW

The countermeasure reference tables are divided into six columns. Column one, "Defense Layer," corresponds to the facility area under evaluation and the current ordinal step. Refer to Section 2.7.2 for descriptions of all the defense layer elements in the reference tables. Column two, "SCM," is the sequential countermeasure number. Column three, "Physical security countermeasure," describes the types of countermeasures associated with the defense layer. Column four, "Appendix A section(s)," links the physical security countermeasure to the corresponding countermeasure description section in Appendix A. Column five, "Delta Difficulty," is the precalculated degree of difficulty to compromise the countermeasure associated with the SCM number based on the Foster–Wallace Formula. Column 6, "Facility

Table B-1. Water Facility Type and Size to Recommended MDT.

Water facilities	Wastewater/stormwater facilities	Recommended MDT ordinal steps
WTP (population > 100k*)	WWTP/SWTP (population > 100k)	6
WTP (pop. served 50–100k)	WWTP/SWTP (pop. served 50–100k)	5 to 6
WTP (pop. served < 3,300)	WWTP/SWTP (pop. served < 3,300k)	4 to 6
Raw water facilities	Collection systems	4 to 6
Wells and pumping stations	Pumping stations	4 to 6
System support facilities	System support facilities	4 to 6
Finished water storage		4 to 6
Water distribution systems		4 to 6

*The symbol k is used to designate 1,000.
Notes: WTP: water treatment plant, WWTP: wastewater treatment plant, SWTP: stormwater treatment plant.

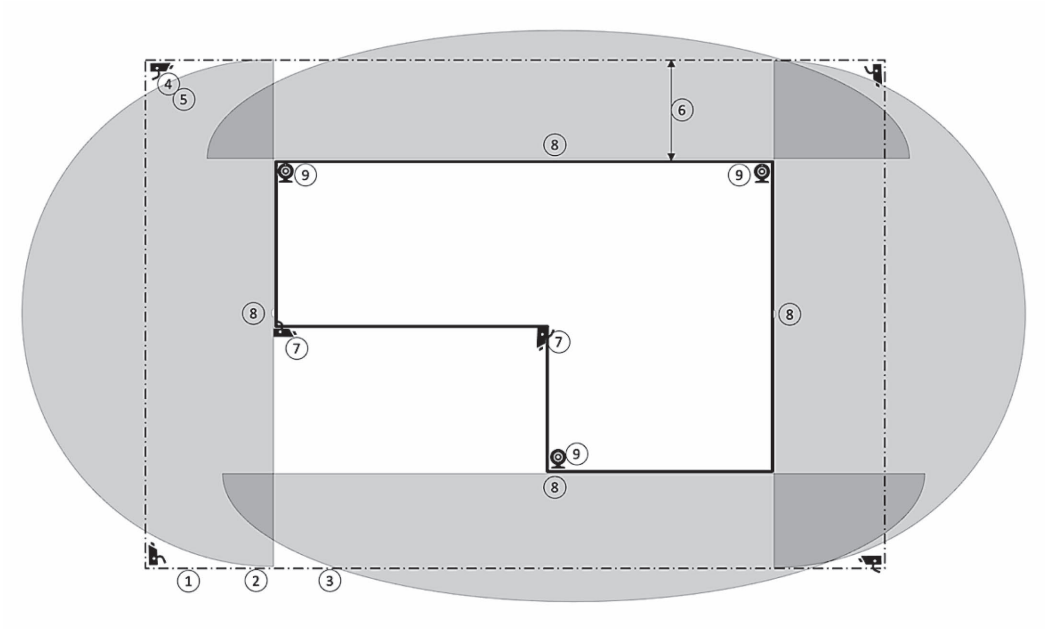
Table B-2. Water Facility and Attack Vector Countermeasure Reference Table Matrix.

	Attack vectors				
Water sector facility types	**AOF***	**VRB***	**VBIED plus VRB***	**Maritime***	**UAS***
WTP/WWTP/SWTP (Population served >500k)	Table B-3	Table B-8	Table B-8	Table B-15	Content for this section is being researched and currently under development and is targeted for a subsequent release.
WTP/WWTP/SWTP (Population served >100k)	Table B-3	Table B-9	Table B-13 Table B-14	Table B-15	
WTP/WWTP/SWTP (Population served 50–100k)	Table B-3 Table B-4	Table B-9 Table B-10	Table B-13 Table B-14	Table B-15	
WTP/WWTP/SWTP (Population served <3,300)	Table B-4 Table B-5	Table B-10 Table B-11	Table B-13 Table B-14	Table B-15	
Wells and pumping stations	Table B-3 Table B-4 Table B-5	Table B-9 Table B-10 Table B-11	Table B-13 Table B-14	Table B-15	
System support facilities	Table B-3 Table B-4 Table B-5	Table B-9 Table B-10 Table B-11	Table B-13 Table B-14	Table B-15	
Finished water storage with controlled access • Aboveground tanks • Elevated tanks • Covered reservoirs	Table B-6	Table B-9 Table B-10 Table B-11	Table B-13 Table B-14	Table B-15	
Finished water storage with public access • Covered reservoirs	Table B-6	Table B-12	Table B-13 Table B-14	Table B-15	
Raw water facilities, collection systems, and Water distribution systems with controlled access	Table B-6	Table B-9 Table B-10 Table B-11 Table B-12	Table B-13 Table B-14	Table B-15	
Raw water facilities with Public access: • Intakes • Dams • Dam appurtenances • Storage lakes	Table B-7	Table B-9 Table B-10 Table B-11 Table B-12	Table B-13 Table B-14	Table B-15	

*AOF: Adversary on Foot attack vector, VRB: Vehicle Ramming Breach attack vector, VBIED: Vehicle Borne Improvised Explosive Device attack vector, Maritime: Maritime attack vector, UAS: Unmanned (Uncrewed) Aircraft System attack vector.

Difficulty," is blank and is intended for the analyst to fill in the delta difficulty value for the facility under evaluation based on the path analysis. Refer to Section 3.6 for details on this process.

The typical drawing in Figure B-1 exhibits the general application of the first nine sequential countermeasures to defend a facility against an adversary on foot attack vector according to cumulative defense strategy. The countermeasure reference tables for adversary on foot attack vectors are similar for the first three defense layers including perimeter, detection line, and observation zone. Refer to the typical drawings associated with the countermeasure reference tables for specifics on Defense Layer elements 4, 5, and 6.



Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0
3 Observation zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	6.0
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	9.0
	8	Tracking device (Ground radar, thermal imagery, etc.)	7.0
	9	PTZ surveillance camera (Day/night coordinated with tracking device)	9.0

Figure B-1. Typical drawing of Defense Layers 1, 2, and 3 for Tables B-3, B-4, and B-5 WTP/WWTP/SWTP, wells and pumping stations, system support facilities adversary on foot.

Note: Diagram numbers correspond to SCM numbers in Tables B-3, B-4, and B-5.

Table B-3. WTP/WWTP/SWTP, Wells and Pumping Stations, System Support Facilities Adversary on Foot with Six Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	2.06×10^{-13} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	1.31×10^{-8} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	8.63×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0004	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.0063	
3 Observation zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	6.0	0.0162	
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	9.0	0.1171	
	8	Tracking device (Ground radar, thermal imagery, etc.)	7.0	0.4423	
	9	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	1.2262	
4 Facility exterior	10	Emergency annunciator (PA system, 2-way audio, alarm, lighting, etc.)	11.0	1.4413	
	11	Intrusion detection (Glass break, motion, analytic, etc.)	7.0	3.9699	
	12	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	6.4198	
	13	Hardened exterior and access point(s) (Steel doors, film on glass, concrete walls, etc.)	10.0	8.9311	
	14	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	8.0	10.9285	
5 Facility interior	15	Unified VMS (Link sites, push scenes, send out notifications, etc.)	9.0	9.7004	
	16	Hardened interior and access point(s) (Steel door, solid wall beyond drop ceiling, etc.)	10.0	12.1317	
	17	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	10.0	11.2131	
	18	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	9.5686	
	19	Intrusion detection (Glass break, motion sensor, etc.)	7.0	7.6017	
	20	Dual-factor authentication PACS secure (PACS secure + access code)	8.0	5.6622	
6 Critical asset ingress	21	Hardened interior and access point(s) (Steel door, solid wall beyond drop ceiling, etc.)	10.0	3.7454	
	22	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	8.0	2.7408	
	23	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	1.7403	
	24	Intrusion detection (Camera analytic, thermal, etc.)	9.0	1.0563	
	25	Dual-factor authentication PACS secure (PACS secure + access code)	8.0	0.6152	
	26	Secondary intrusion detection (Glass break, motion sensor, etc.)	7.0	0.3448	
	27	Multifactor Authentication (MFA) PACS secure (PACS secure + access code + biometric)	8.0	0.1865	
				Sum of Facility Difficulty values	

Note: Table references Figures B-1 and B-2.

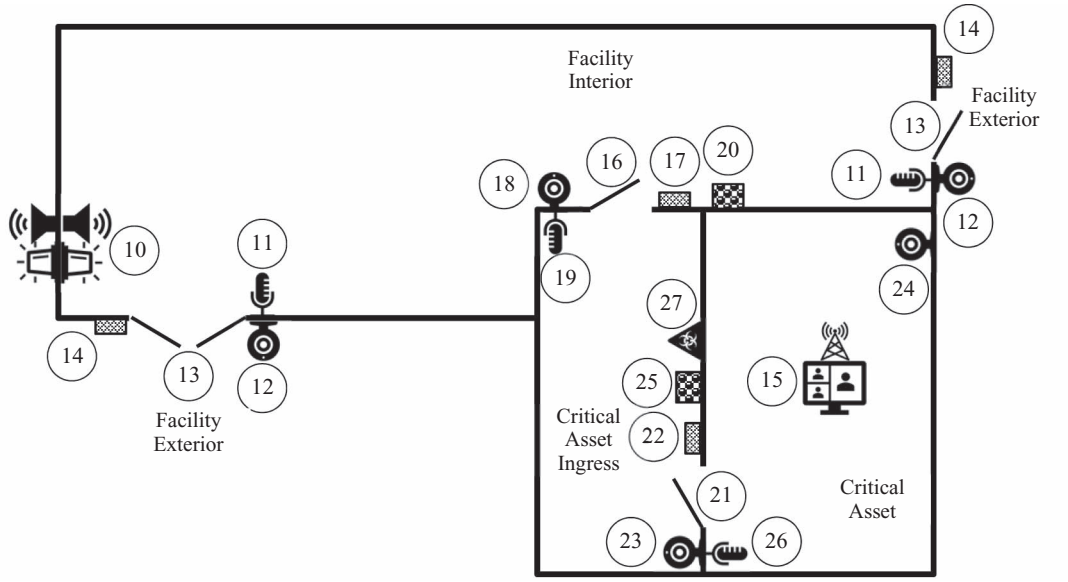


Figure B-2. Typical drawing of Defense Layers 4, 5, and 6 for Table B-3 WTP/WWTP/SWTP, wells and pumping stations, system support facilities adversary on foot with six ordinal steps.

Note: Diagram numbers correspond to SCM numbers in Table B-3.

Table B-4. WTP/WWTP/SWTP, Wells and Pumping Stations, System Support Facilities Adversary on Foot with Five Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	3.36×10^{-11} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	1.33×10^{-6} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	0.0007	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0195	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1961	
3 Observation zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	6.0	0.4407	
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	9.0	2.0843	
	8	Tracking device (Ground radar, thermal imagery, etc.)	7.0	5.1560	
	9	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	9.3618	
4 Facility exterior	10	Unified VMS (Link sites, push scenes, send out notifications, etc.)	9.0	9.6774	
	11	Hardened exterior and access point(s) (Steel doors, film on glass, concrete walls, etc.)	10.0	15.4721	
	12	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	8.0	15.8275	
	13	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	13.9023	
	14	Intrusion detection (Glass break, motion, analytic, etc.)	7.0	10.7147	
5 Critical asset ingress	15	Hardened interior and access point(s) (Steel door, solid wall beyond drop ceiling, etc.)	10.0	6.8185	
	16	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	8.0	4.8375	
	17	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	2.7609	
	18	Intrusion detection (Glass break, motion sensor, camera analytic, etc.)	7.0	1.4539	
	19	Dual-factor authentication PACS secure (PACS secure + access code)	8.0	0.7125	
	20	Emergency annunciator (PA system, 2-way audio, alarm, lighting, etc.)	11.0	0.3274	
				Sum of Facility Difficulty values	

Note: Table references Figures B-1 and B-3.

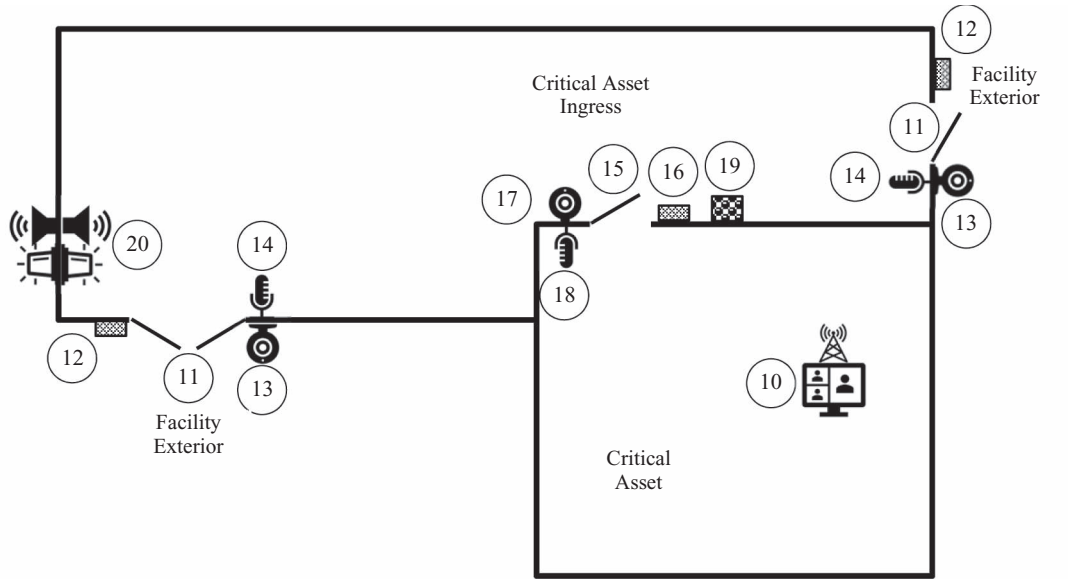


Figure B-3. Typical drawing of Defense Layers 4 and 5 for Table B-4 WTP/WWTP/SWTP, wells and pumping stations, system support facilities adversary on foot with five ordinal steps.

Note: Diagram numbers correspond to SCM numbers in Table B-4.

Table B-5. WTP/WWTP/SWTP, Wells and Pumping Stations, System Support Facilities Adversary on Foot with Four Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	7.05×10^{-18} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	5.76×10^{-10} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	2.10×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	
3 Observation zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	6.0	0.7349	
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	9.0	4.8853	
	8	Tracking device (Ground radar, thermal imagery, etc.)	7.0	14.0142	
	9	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	23.1013	
4 Critical asset ingress	10	Hardened exterior and access point(s) (Steel doors, film on glass, concrete walls, etc.)	10.0	21.6223	
	11	PACS secure 13.56 MHz (PACS 125 kHz not acceptable)	8.0	19.1052	
	12	Unified VMS (Link sites, push scenes, send out notifications, etc.)	9.0	10.3558	
	13	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	4.2298	
	14	Intrusion detection (Glass break, motion sensor, camera analytic, etc.)	7.0	1.3534	
				Sum of Facility Difficulty values	

Note: Table references Figures B-1 and B-4.

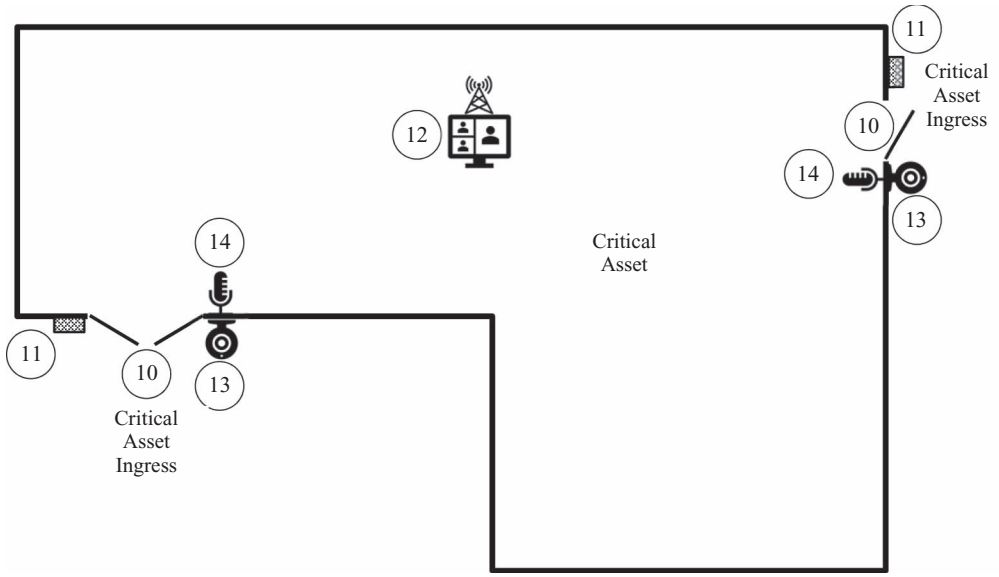


Figure B-4. Typical drawing of Defense Layer 4 for Table B-5 WTP/WWTP/SWTP, wells and pumping stations, system support facilities adversary on foot with four ordinal steps.
Note: Diagram numbers correspond to SCM numbers in Table B-5.

Table B-6. Finished Water Storage Facilities with Controlled and Public Access, Raw Water Facilities, and Collection Systems with Controlled Access Adversary on Foot with Four Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	7.05×10^{-18} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	5.76×10^{-10} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	2.10×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	
3 Observation zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	6.0	0.7349	
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	9.0	4.8853	
	8	Tracking device (Ground radar, thermal imagery, etc.)	7.0	14.0142	
	9	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	23.1013	
4 Critical asset ingress	10	Hardened exterior and access point(s) (Steel doors, film on glass, concrete walls, etc.)	10.0	21.6223	
	11	Hardened access control (PACS secure, hidden shackle padlock w/shield, etc.)	8.0	19.1052	
	12	Surveillance camera dedicated to access point(s) (Detection analytic, virtual trip wire, etc.)	9.0	10.3558	
	13	Intrusion detection (Vibration, motion, seismic, fiberoptic, etc.)	7.0	4.2298	
	14	Emergency annunciator (PA system, 2-way audio, alarm, lighting, etc.)	11.0	1.3534	
				Sum of Facility Difficulty values	

Note: Table references Figure B-5.

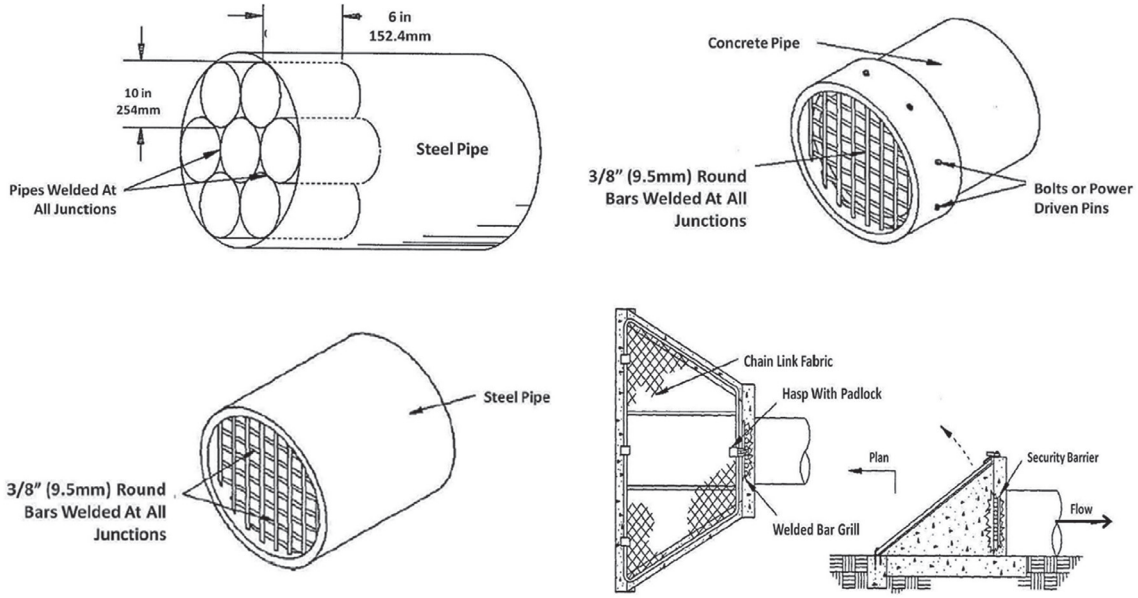


Figure B-5. Typical drawing of SCM 10 for Table B-6 raw water facilities, collection systems, and water distribution systems with controlled access adversary on foot with four ordinal steps.

Source: Adapted from UFC 4-022-03 (US DOD 2013).

Table B-7. Raw Water Facilities with Public Access Adversary on Foot with Four Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	7.05×10^{-18} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	5.76×10^{-10} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	2.10×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	
3 Observation zone	6	Open space between detection line and facility [250 ft (76.2 m) for 20 s delay]	6.0	0.7349	
	7	Surveillance camera dedicated to observation zone (Day/night, detection analytic, virtual trip wire, etc.)	9.0	4.8853	
	8	Tracking device (Ground radar, thermal imagery, etc.)	7.0	14.0142	
	9	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	23.1013	
4 Critical asset ingress	10	Unified VMS (Link sites, push scenes, send out notifications, etc.)	9.0	21.6223	
	11	Tactical Deterrence (Human capital, LRAD, targeted illumination, etc.)	12.0	19.1052	
	12	Long-range tracking device (Ground radar, thermal imagery, etc.)	7.0	10.3558	
	13	Long-range PTZ surveillance camera (Day/night coordinated with tracking device)	9.0	4.2298	
	14	Emergency annunciator (PA system, 2-way audio, alarm, lighting, etc.)	11.0	1.3534	
				Sum of Facility Difficulty values	

Table B-8. VBIED Including VRB, Sallyport Vehicle Entry with Six Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	2.06×10^{-13} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	1.31×10^{-8} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	8.63×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0004	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.0063	
3 Approach zone	6	Tracking device (Ground radar, thermal imagery, etc.)	7.0	0.0162	
	7	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	0.1171	
	8	Exterior speed reduction (Reverse pitch corner, limited straightaways, etc.)	5.0	0.4423	
	9	Full perimeter vehicle barrier (Barrier, bollards, trench, natural terrain, etc.)	1.0, 5.0	1.2262	
4 Primary gate	10	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	1.4413	
	11	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	3.9699	
	12	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	6.4198	
	13	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	8.9311	
	14	K/M-Rated entry and exit traffic flow separation (K/M-Rated barriers, berms, structures, etc.)	5.0	10.9285	
5 Sallyport	15	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	9.7004	
	16	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	12.1317	
	17	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	11.2131	
	18	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	9.5686	
	19	K/M-Rated barrier enclosed sallyport inspection area (Consistent with perimeter fence + K/M-rated barriers)	5.0	7.6017	
	20	Tactical Deterrence (Human capital, etc.)	12.0	5.6622	
6 Facility exterior	21	K/M-Rated interior speed reduction (Reverse pitch corner, K/M-rated staggered barriers)	5.0	3.7454	
	22	K/M-Rated vehicle crash barrier at critical area entry (Active K/M-Rated bollards or crash barrier, etc.)	5.0	2.7408	
	23	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	1.7403	
	24	K/M-Rated barriers limiting critical area access (One entry/exit to critical area, etc.)	5.0	1.0563	
	25	Parking lot standoff distance from facility (Standoff distance based on detonation pressure)	5.0	0.6152	
	26	K/M-Rated barriers between building and parking lot (K/M-Rated barriers, berms, structures, etc.)	5.0	0.3448	
	27	Blast rated facility exterior (Doors, windows, wall structure, etc.)	10.0	0.1865	
				Sum of Facility Difficulty values	

Note: Table references Figure B-6.

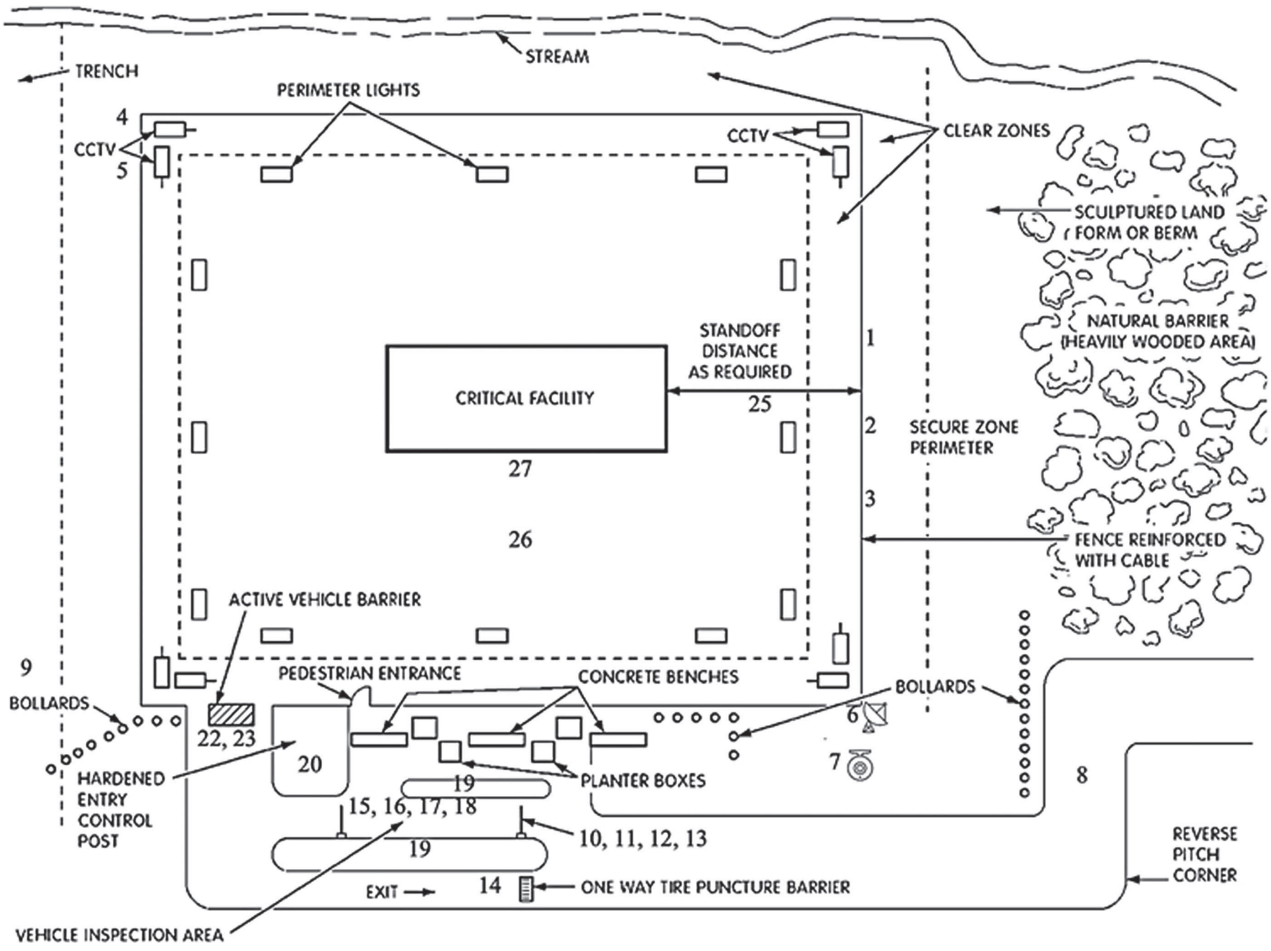


Figure B-6. Typical drawing for Table B-8 VBIED including VRB with six ordinal steps.

Source: Adapted from UFC 4-022-02 (US DOD 2010b).

Note: Diagram numbers correspond to SCM numbers in Table B-8.

Table B-9. Vehicle Ramming Breach, Sallyport Vehicle Entry with Five Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	3.36×10^{-11} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	1.33×10^{-6} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	0.0007	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0195	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1961	
3 Approach zone	6	Tracking device (Ground radar, thermal imagery, etc.)	7.0	0.4407	
	7	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	2.0843	
	8	Exterior speed reduction (Reverse pitch corner, limited straightaways, etc.)	5.0	5.1560	
	9	Full perimeter vehicle barrier (Barrier, bollards, trench, natural terrain, etc.)	1.0, 5.0	9.3618	
4 Primary gate	10	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	9.6774	
	11	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	15.4721	
	12	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	15.8275	
	13	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	13.9023	
	14	K/M-Rated entry and exit traffic flow separation (K/M-Rated barriers, berms, structures, etc.)	5.0	10.7147	
5 Sallyport	15	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	6.8185	
	16	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	4.8375	
	17	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	2.7609	
	18	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	1.4539	
	19	K/M-Rated barrier enclosed sallyport inspection area (Consistent with perimeter fence + K/M-rated barriers)	5.0	0.7125	
	20	Tactical Deterrence (Human capital, etc.)	12.0	0.3274	
				Sum of Facility Difficulty values	

Table B-10. Vehicle Ramming Breach, Sallyport Vehicle Entry with Four Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	7.05×10^{-18} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	5.76×10^{-10} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	2.10×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	
3 Primary gate	6	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	0.7349	
	7	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	4.8853	
	8	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	14.0142	
	9	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	23.1013	
4 Sallyport	10	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	21.6223	
	11	PACS entry system (PACS secure + intercom + dedicated gate camera)	8.0	19.1052	
	12	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	10.3558	
	13	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	4.2298	
	14	K/M-Rated barrier enclosed sallyport inspection area (Consistent with perimeter fence + K/M-rated barriers)	5.0	1.3534	
				Sum of Facility Difficulty values	

Table B-11. Vehicle Ramming Breach, Single Gate Vehicle Entry with Four Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	7.05×10^{-18} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	5.76×10^{-10} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	2.10×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	
3 Approach zone	6	Tracking device (Ground radar, thermal imagery, etc.)	7.0	0.7349	
	7	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	4.8853	
	8	Exterior speed reduction (Reverse pitch corner, limited straightaways, etc.)	5.0	14.0142	
	9	Full perimeter vehicle barriers (Barriers, bollards, trench, natural terrain, etc.)	5.0	23.1013	
4 Primary gate	10	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	21.6223	
	11	PACS entry system (PACS secure + intercom + gate camera)	8.0	19.1052	
	12	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	10.3558	
	13	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	4.2298	
	14	K/M-Rated interior speed reduction barriers (K/M-Rated staggered barriers, tight corners, etc.)	5.0	1.3534	
				Sum of Facility Difficulty values	

Table B-12. Vehicle Ramming Breach, Finished Water Storage with Public Access Single Gate Vehicle Entry with Four Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, post and chain, split rail, etc.)	1.0	7.05×10^{-18} small number	
	2	Posting of perimeter boundary and lighting [No Unauthorized Vehicle signs every 50 ft (15.24 m)]	3.0, 4.0	5.76×10^{-10} small number	
2 Detection line	3	Perimeter detection (Seismic, fiberoptic, microwave, etc.)	7.0	2.10×10^{-6} small number	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	
3 Approach zone	6	Tracking device (Ground radar, thermal imagery, etc.)	7.0	0.7349	
	7	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	4.8853	
	8	Exterior speed reduction (One entry/exit, tight access width, sharp turns, etc.)	5.0	14.0142	
	9	Full perimeter vehicle barriers (Barriers, bollards, trench, natural terrain, etc.)	5.0	23.1013	
4 Primary gate/critical asset ingress	10	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	21.6223	
	11	Hardened access control entry system (Access control + intercom + dedicated camera)	8.0	19.1052	
	12	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	10.3558	
	13	K/M-Rated vehicle barriers (active or passive) (K/M-Rated active barriers, removable bollards, etc.)	2.0	4.2298	
	14	K/M-Rated interior speed reduction barriers (K/M-Rated staggered barriers, tight corners, etc.)	5.0	1.3534	
				Sum of Facility Difficulty values	

Table B-13. VBIED Including VRB, Sallyport Vehicle Entry with Five Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	3.36×10^{-11} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	1.33×10^{-6} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	0.0007	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0195	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1961	
3 Primary gate	6	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	0.4407	
	7	PACS entry system (PACS secure + intercom + dedicated gate camera)	8.0	2.0843	
	8	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	5.1560	
	9	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	9.3618	
4 Sallyport	10	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	9.6774	
	11	PACS entry system (PACS secure + intercom + dedicated gate camera)	8.0	15.4721	
	12	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	15.8275	
	13	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	13.9023	
	14	K/M-Rated barrier enclosed sallyport inspection area (Consistent with perimeter fence + K/M-rated barriers)	5.0	10.7147	
5 Facility exterior	15	K/M-Rated vehicle crash barrier at critical area entry (Active K/M-Rated bollards or crash barrier, etc.)	5.0	6.8185	
	16	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	4.8375	
	17	K/M-Rated interior speed reduction (Reverse pitch corner, K/M-rated staggered barriers)	5.0	2.7609	
	18	Parking lot standoff distance from facility (Standoff distance based on detonation pressure)	5.0	1.4539	
	19	K/M-Rated barriers between building and parking lot (K/M-Rated barriers, berms, structures, etc.)	5.0	0.7125	
	20	Blast rated facility exterior (Doors, windows, wall structure, etc.)	10.0	0.3274	
				Sum of Facility Difficulty values	

Note: Table references Figure B-7.

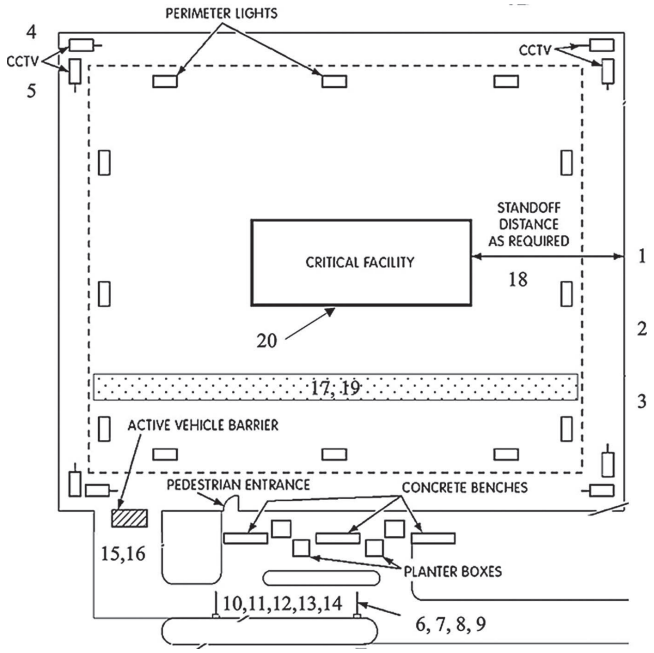


Figure B-7. Typical drawing for Table B-13 VBIED including VRB with five ordinal steps.

Source: Adapted from UFC 4-022-02 (US DOD 2010b).

Note: Diagram numbers correspond to SCM numbers in Table B-13.

Table B-14. VBIED Including VRB, Single Gate Vehicle Entry with Five Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Fence, wall, barrier, etc.)	1.0	3.36×10^{-11} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs every 50 ft (15.24 m), etc.]	3.0, 4.0	1.33×10^{-6} small number	
2 Detection line	3	Perimeter detection (Copper, fiberoptic, contact, microwave, etc.)	7.0	0.0007	
	4	Surveillance camera dedicated to detection line (Detection analytic, virtual trip wire, etc.)	9.0	0.0195	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1961	
3 Approach zone	6	Tracking device (Ground radar, thermal imagery, etc.)	7.0	0.4407	
	7	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	2.0843	
	8	Exterior speed reduction (Reverse pitch corner, limited straightaways, etc.)	5.0	5.1560	
	9	Full perimeter vehicle barrier (Barrier, bollards, trench, natural terrain, etc.)	1.0, 5.0	9.3618	
4 Primary gate	10	Manual gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	9.6774	
	11	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	15.4721	
	12	Automated gate consistent with perimeter fencing (Single hung, double hung, sliding, etc.)	2.0	15.8275	
	13	K/M-Rated automated gate consistent with fencing (Single hung, double hung, sliding, etc.)	2.0	13.9023	
	14	K/M-Rated entry and exit traffic flow separation (K/M-Rated barriers, berms, structures, etc.)	5.0	10.7147	
5 Facility exterior	15	K/M-Rated vehicle crash barrier at critical area entry (Active K/M-Rated bollards or crash barrier, etc.)	5.0	6.8185	
	16	PACS entry system (PACS secure + intercom + dedicated camera)	8.0	4.8375	
	17	K/M-Rated interior speed reduction (Reverse pitch corner, K/M-rated staggered barriers)	5.0	2.7609	
	18	Parking lot standoff distance from facility (Standoff distance based on detonation pressure)	5.0	1.4539	
	19	K/M-Rated barriers between building and parking lot (K/M-Rated barriers, berms, structures, etc.)	5.0	0.7125	
	20	Blast rated facility exterior (Doors, windows, wall structure, etc.)	10.0	0.3274	
				Sum of Facility Difficulty values	

Table B-15. Maritime Attack with Four Ordinal Steps.

Defense Layer	SCM	Physical Security Countermeasure	Appendix A Sections	Delta Difficulty %	Facility Difficulty %
1 Perimeter	1	Perimeter establishment (Buoys marking restricted area)	1.0	7.05×10^{-18} small number	
	2	Posting of perimeter boundary and lighting [No Trespass signs on buoys every 50 ft (15.24 m)]	3.0, 4.0	5.76×10^{-10} small number	
2 Detection line	3	Surface and subsurface detection (Marine net, fiberoptic netting/barrier, etc.)	7.0	2.10×10^{-6} small number	
	4	Underwater detection (Diver and watercraft sonar detection analytic)	7.0	0.0045	
	5	Day/Night surveillance dedicated to detection line (Detection analytic, thermal fence, etc.)	9.0	0.1516	
3 Observation zone	6	Open space between detection line and facility (Distance corresponds with detection range)	6.0	0.7349	
	7	Long-range surveillance camera (Thermal or cooled thermal imagery device, etc.)	9.0	4.8853	
	8	Long-range tracking device (Long-range radar or thermal system, etc.)	7.0	14.0142	
	9	PTZ surveillance camera (Day/night camera coordinated with tracking device)	9.0	23.1013	
4 Facility exterior	10	Hardened barrier on the water (Net boat barriers, defensive buoy, etc.)	5.0	21.6223	
	11	Hardened access (Anti-climb surface, barriers, fencing, etc.)	1.0, 5.0, 10.0	19.1052	
	12	Unified VMS (Link sites, push scenes, send out notifications, etc.)	9.0	10.3558	
	13	Tactical Deterrence (LRAD, flood light coordinated with radar, etc.)	12.0	4.2298	
	14	Tactical Deterrence (Human capital, dogs, etc.)	12.0	1.3534	
				Sum of Facility Difficulty values	

This page intentionally left blank

APPENDIX C
SYSTEM FACILITIES SCOPE AND MISSION

C.1 INTRODUCTION

Appendix C details the scope and mission (ASCE 2010b, c) of the water facilities listed in Table 2-1 of Chapter 2. ASCE/AWWA/WEF (2006a, b) provided the scope, facility mission, philosophy of security approach, and benchmark security measures during the drafting for the American National Standards for Trial Use, and this appendix only provides the scope and mission sections of that material without providing the DBT approach sections as developed in 2006. The more recent approach of Chapters 2 and 3 uses the application tables provided in Appendix B as indicated earlier. The references within these Appendix C sections have been updated with the most recent appropriate information in References.

C.2 WATER TREATMENT PLANTS

C.2.1 Scope This guideline covers water treatment plants used within a municipal drinking water system. Protection considerations should include damage or destruction of individual treatment processes or equipment, or introduction of a chemical, radiological, or biological agent that contaminates the drinking water supply or renders the facilities unusable. Employee safety and public health concerns can be caused by the intentional release of hazardous chemicals or toxic gases or by damaging ventilation and other life-safety control features. The potential for malevolent individuals to create intentional fire and explosive hazards may be additional concerns requiring security features.

C.2.2 Mission The mission of this facility is to treat source water to drinking water standards. Water treatment plants may produce from 100,000 gal. (380 m^3) to 100 million gal. (1,140,000 m^3)/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 clear well 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 public, these facilities can be in residential settings or amid denser populated urban areas. Because of safety concerns, the public generally has no direct access. More detailed information on specific functions and treatment processes is contained in *Water Treatment Plant Design* (AWWA/ASCE 2012).

A water treatment facility may have chemical injection facilities downstream of clear well storage to adjust and maintain the chemical attributes of the finished water. These chemical facilities (chemical supply lines and metering equipment) may be outside of the boundary of the water treatment plant campus but should be treated using similar security measures to those recommended for the treatment plant perimeter and facilities.

Special considerations should be provided for security of extremely critical assets or facilities such as in-plant pumping stations, main electrical switchgear, emergency generators, disinfection systems, or SCADA/security computer equipment. Special security considerations should also be provided for water treatment plants that store large volumes of hazardous or toxic chemicals, such as chlorine or ammonia gas. Extremely critical or hazardous assets may require additional security measures.

C.3 RAW WATER FACILITIES

C.3.1 Scope This guideline covers raw water facilities that are components of a municipal drinking water system and are under the control of the utility. It is limited to surface raw water facilities: river and lake intakes, pipelines and canals that are used to convey raw water, valve vaults and control structures used on these transmission lines and structures, and other facilities upstream of the treatment plant.

A dam is commonly a raw water facility that may be under the control of a utility. 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.

C.3.2 Mission The mission of this type of facility is to provide a supply of water to treatment plants. The facilities include storage reservoirs, basins, intakes, pipelines, and vaults (meter, valve, etc.). In general, these facilities are not continuously staffed. They may be visited periodically by staff who check the facilities, perform maintenance activities, conduct raw water monitoring, and respond to alarms. The facilities are often isolated from the 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 used.

Special considerations may be warranted for the following:

- 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; and

- Raw water intakes/supplies for systems without barriers, such as watersheds whose water is delivered to the public without filtration or typical treatment.

C.4 WELLS AND PUMPING STATIONS

C.4.1 Scope This guideline covers water wells and pumping stations used within a water system. It discusses security features for protecting wells or booster pumping stations. Additional assets for consideration could 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.

C.4.2 Mission The mission of a well facility is to withdraw groundwater from an aquifer to be used as drinking water supply. In general, operations and maintenance staff periodically visit these facilities to perform maintenance and inspection/monitoring activities or to respond to failure alarms. These facilities may be isolated from the public or located in residential, parklike settings or amid denser populated urban areas. Multiple wells can be found at one location, and well facilities are often collocated with storage tanks or other utility-owned infrastructure such as maintenance buildings.

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

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

More detailed information on wells can be found in AWWA A100-20, *Water Wells* (AWWA 2020b). More detailed information on pumping stations can be found in *Pumping Station Design* (Jones et al. 2005).

C.5 WATER SYSTEM SUPPORT FACILITIES

C.5.1 Scope This section presents a guideline for security for support facilities that are part of municipal drinking water systems. Water system support facilities include administrative buildings, maintenance yards, sites for material and vehicle storage, and laboratories.

C.5.2 Mission The common element linking these facilities is that they may not be in direct contact with the drinking water. If a facility such as a laboratory or storage yard is located at a water treatment plant, then the security guideline for water treatment plants should be referenced. This guideline applies to those facilities that are not located at a water treatment plant, water pumping station, or intake facility, or otherwise in direct contact with 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 numbers of people entering and leaving the facility, including the public;
- High vehicle traffic;
- Fuel tanks to supply the utility fleet;
- Storage for utility vehicles that, as moving assets, present unique challenges;
- In the case of laboratories, many household chemicals or even pathogens that are used in tests;
- May be symbolic of the utility's image, such as a headquarters facility; and
- May be combined with other government facilities, such as an administrative facility within the city hall or a maintenance yard combined with other city maintenance functions.

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

Special considerations should be provided for security of extremely critical assets or facilities such as water quality laboratories; SCADA; EOCs; centralized security monitoring centers; security equipment; network computer servers, hubs, and related systems; and dangerous chemicals and pathogens located in analytical laboratories. Special consideration should also be provided for sites that have an intended public open space/access focus, such as headquarters complexes.

C.6 FINISHED WATER STORAGE FACILITIES

C.6.1 Scope This section of the guidelines covers water storage tanks and finished water reservoirs used within a potable water distribution system. 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.

C.6.2 Mission The mission of this facility is to store potable water for distribution to customers. Storage is needed to meet daily flow fluctuations and to supply firefighting and emergency needs. Three types of potable water storage are typically used in the water industry: aboveground water storage tanks, elevated tanks, and covered reservoirs. Aboveground water storage tanks are constructed of concrete, steel, FRP, or wood with the tank floor situated at grade (i.e., 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 by a ladder or system of ladders. Covered, finished water reservoirs may be slightly larger and are often constructed below grade but with access and vents at or above grade.

Usually, these facilities are not staffed, and operations and maintenance personnel visit the sites infrequently to perform maintenance activities or to respond to failure alarms. The tanks and reservoirs are often located in residential, parklike settings or sometimes have tennis courts painted on top of them where the public has access to the tank. Direct public access to finished water tanks is not desirable from a security point of view. In other cases, the tanks are isolated from public access. Potable water storage facilities at more remote locations within a distribution system may be provided with chemical facilities (chlorine and/or ammonia) to maintain the chemical attributes of finished water as it progresses through the distribution system. Measures to address chemical facilities are presented in Section C.2, "Water Treatment Plants," and are not included here.

AWWA Manual M42, *Steel Water-Storage Tanks* (AWWA 1998) and D100-11, *Welded Carbon Steel Tanks for Water Storage* (AWWA 2011) provide additional information on the

design and function of steel water storage tanks. Concrete tank standards and information are provided in AWWA D110-13(R18), *Wire- and Strand-Wound, Circular, Prestressed Concrete Water Tanks* (AWWA 2018), AWWA D115-20, *Circular Prestressed Concrete Water Tanks with Circumferential Tendons* (AWWA 2020a), and ACI PRC-371-16, *Guide for the Analysis, Design, and Construction of Elevated Concrete and Composite Steel-Concrete Water Storage Tanks* (ACI 2016). FRP tanks are covered in AWWA D120-19, *Thermosetting Fiberglass-Reinforced Plastic Tanks* (AWWA 2019).

C.7 WATER DISTRIBUTION SYSTEMS

C.7.1 Scope This section of the guidelines covers the water distribution system component of municipal drinking water systems. 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.

C.7.2 Mission The mission of these systems is to distribute drinking water to the customers of the system. Water distribution systems can cover many square miles (kilometers) in an area. They include pipelines, isolation and control valves, hydrants, customer meters, backflow valves, air release valves, pressure-reducing valves, small chemical storage and injection facilities, and related items (Mays 2000). As the name suggests, these facilities are distributed throughout the community that is served by the water system and rarely have defined facility perimeters. Most pipelines and valves are buried and therefore are out of sight of the public. However, appurtenances and the structures enclosing them, such as air valve vaults and the like, are sometimes aboveground and visible. Furthermore, every customer has a direct connection to the system through their service line. Other sections of these guidelines cover finished water storage facilities, pumping stations, and chemical facilities (see Section C.2.2 for chemical facilities).

C.8 WASTEWATER/STORMWATER TREATMENT PLANTS

C.8.1 Scope This guideline covers wastewater treatment plants used within a municipal wastewater system. It includes damage or destruction of individual treatment processes or equipment, or introduction of a chemical, radiological, or biological contaminant that severely impedes wastewater treatment or renders the facilities unusable. A wastewater treatment plant that cannot provide adequate capacity or performance because of a malevolent activity could discharge an effluent with significantly impaired quality that may create a public health hazard or cause environmental damage of the downstream receiving water or receiving environment. Employee safety and public health concerns can be caused by the intentional release of hazardous chemicals or toxic gases or by damaging ventilation and other life-safety control features. The potential for malevolent individuals to create intentional fire and explosive hazards are additional concerns that may require security features.

C.8.2 Mission The mission of this type of facility is to treat the incoming wastewater to an environmentally and public-health-acceptable level before discharging to a receiving body of water or other system. Wastewater treatment plants typically include below-grade, ground level, and elevated structures, tankage, and buildings with typical throughput capacities ranging from 1,000 gal./day (3.8 m^3/day) to more than 1 billion gal./day (>3,800,000 m^3/day). Large wastewater treatment plants are routinely staffed on a continuous basis; small facilities are likely to be staffed by operations and maintenance personnel only periodically to perform maintenance activities, conduct process monitoring, collect environment samples, or respond to failure alarms. Although often isolated from the public, these facilities can be in residential settings or amid denser populated urban areas. Because of safety concerns, the public generally has no direct access.

More detailed information on specific functions and treatment processes is contained in the WEF Manual of Practice No. 8, *Design of Municipal Wastewater Treatment Plants*, 4th Edition [WEF 2010; this is the same as ASCE MOP 76 (ASCE 2010a)], and WEF Manual of Practice No. 11, *Operation of Municipal Wastewater Treatment Plants*, 6th Edition (WEF 2005).

Typical critical assets of wastewater treatment plants that should be considered for more robust or enhanced security measures include

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

C.9 COLLECTION SYSTEMS

C.9.1 Scope This guideline covers the collection and conveyance components of wastewater and stormwater systems. It includes damage or destruction of individual facilities or equipment, release of untreated wastewater into the environment, or use of the collection system as a conduit to reach buildings or other targets of malevolent action.

C.9.2 Mission The mission of these facilities is to collect and convey wastewater from its origins in the community to wastewater treatment facilities or to convey stormwater to treatment or to discharge points. They include pipelines, culverts, conveyance tunnels, manholes, isolation and control valves, air release valves, combined sewer structures, stormwater inlets and catch basins, stormwater outfall structures, stormwater retention/detention basins, and related items. These facilities are distributed throughout the community that is served by the utility and rarely have defined individual facility perimeters. Most pipelines and valves are buried and therefore are out of sight of the public. However, every customer has a direct connection to the wastewater system through their service line, and manholes that provide access to the wastewater and stormwater systems are prevalent throughout the community.

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

- *Gravity Sanitary Sewer Design and Construction*, WEF Manual of Practice No. FD-5 and ASCE MOP 60 (WEF 2007, ASCE 2007)
- *Wastewater Collection Systems Management*, Manual of Practice No. 7, 5th Edition (WEF 1999)

- *Design and Construction of Urban Stormwater Management Systems*, WEF Manual of Practice No. FD-20 and ASCE MOP 77 (WEF 1992, ASCE 1992)
- *Standard Guidelines for the Design, Installation, and Operation and Maintenance of Urban Stormwater Systems*, ASCE/EWRI 45-16, 46-16, 47-16 (ASCE 2016)

Collection systems present challenges in developing adequate detection and delay approaches, because many facilities are not constructed with defined perimeters or site areas where access can be controlled and these facilities are frequently open to the public. For the elements of the collection systems without defined perimeters and site areas, a utility may elect to selectively apply the recommended security measures on a subset of their most critical assets.

C.10 PUMPING STATIONS

C.10.1 Scope This guideline covers pumping stations used within a wastewater collection system (often called a sanitary sewer or sewerage system) or within a stormwater system. It includes damage or destruction of the pumping station equipment that causes an uncontrolled release of the wastewater or stormwater creating a public health hazard or environmental damage. Additional threats include introduction of a chemical, radiological, or biological contaminant that severely impedes or damages downstream sewer lines and treatment processes that may ultimately contaminate the water or environmental system receiving the treatment plant's discharge.

C.10.2 Mission The mission of this facility is to pump raw wastewater or stormwater to a treatment facility, another pumping station, or to a sewer line at a higher elevation. Pumping stations typically comprise both below-grade and at-grade facilities with capacities ranging from 1,000 gal./day (3.8 m^3/day) to more than 1 million gal./day (>3,800 m^3/day). Although larger pumping stations may be routinely staffed on a continuous or part-time basis, more frequently operations and maintenance staff only visit these facilities periodically to perform maintenance activities or to respond to failure alarms. Although typically isolated from the public, these facilities can be in residential, parklike settings, or amid denser populated urban areas. Because of safety concerns, the public generally has no direct access.

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

C.11 WASTEWATER/STORMWATER SYSTEM SUPPORT FACILITIES

C.11.1 Scope This guideline presents guidance for security for support facilities that are part of wastewater and stormwater systems. It includes damage or destruction of individual facilities or critical assets within facilities.

C.11.2 Mission Wastewater/stormwater system support facilities include administrative buildings, maintenance yards, sites for material and vehicle storage, laboratories, and septage disposal facilities. The common element linking these facilities is that they are not in direct contact with wastewater or stormwater. In some cases, support facilities are located apart from the water flow and can have a lower risk for being avenues of intentional contamination of the wastewater or stormwater.

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

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

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

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.

REFERENCES

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

ACI (American Concrete Institute). 2016. *Guide for the analysis, design, and construction of elevated concrete and composite steel-concrete water storage tanks*. ACI PRC-371-16. Farmington Hills, MI: ACI. This 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 and consist of a steel water storage tank supported by a cylindrical reinforced concrete pedestal.

ANSI/AWWA (American National Standards Institute and American Water Works Association). 2018a. *Dry-barrel fire hydrants*. AWWA C502-18. Denver: AWWA. Standard AWWA C502-18 can be referenced in specifications for purchasing and receiving dry-barrel fire hydrants for fire protection service and can be used as a guide for evaluating materials and designing, testing, and inspecting dry-barrel fire hydrants.

ANSI/AWWA. 2018b. *Wet-barrel fire hydrants*. C503-18. Denver: AWWA. Standard AWWA C503-18 can be referenced in requirements for purchasing and receiving wet-barrel fire hydrants for fire-protection service and can be used as a guide for inspecting and testing wet-barrel fire hydrants.

ANSI/ISA (International Society of Automation). 2007. *Security for industrial automation and control systems, Part 1-1: Terminology, concepts, and models*. ANSI 62443-1-1. Research Triangle Park, NC: ISA. This guideline covers terminology, concepts, and models for industrial automation and control systems security.

ANSI/NAAMM/HMMA (American National Standards Institute, National Association of Architectural Metal Manufacturers, and Hollow Metal Manufacturers Association). 2013. *Guide specifications for commercial security hollow metal doors and frames*. ANSI/NAAMM/HMMA 862-13. Chicago: NAAMM. This document provides specifications for commercial security hollow metal doors and frames. Its focus is protection from vandalism, forced entry, theft, and firearms attack.

ASCE. 1992. *Design and construction of urban stormwater management systems.* MOP 77. Reston, VA: ASCE. This manual is an update of relevant portions of the ASCE/WPCF, *Design and Construction of Sanitary and Storm Sewers*, MOP 37, to include the new developments in the field of stormwater management. The manual describes currently accepted procedures for financial services, regulations, surveys and investigations, design concepts and master planning, hydrology and water quality, storm drainage hydraulics, and computer modeling.

ASCE. 2007. *Gravity sanitary sewer design and construction.* MOP 60. Reston, VA: ASCE. This manual is the second revision of the relevant portions of the ASCE/WPCF, *Design and Construction of Sanitary and Storm Sewers*, MOP 37, and presents the current practice in the field of sanitary sewer design and construction. Its intended audience is design professionals knowledgeable in the areas of gravity sewers.

ASCE. 2010a. *Design of municipal wastewater treatment plants*. MOP 76. Reston, VA: ASCE. The focus of this manual is current practice in the design of municipal wastewater treatment plants. Its intended audience is design professionals knowledgeable in the areas related to wastewater treatment, including plant operations and regulations.

ASCE. 2010b. *Guidelines for the physical security of wastewater/stormwater utilities*. ANSI/ASCE/EWRI 57-10. Reston, VA: ASCE. This wastewater/stormwater utilities standard recommends physical and electronic security measures for physical protection systems to protect against identified adversaries, referred to as DBTs, with specified motivations, tools, equipment, and weapons.

ASCE. 2010c. *Guidelines for the physical security of water utilities.* ANSI/ASCE/EWRI 56-10, v-57. Reston, VA: ASCE. This water utilities standard recommends physical and electronic security measures for physical protection systems to protect against identified adversaries, referred to as DBTs, with specified motivations, tools, equipment, and weapons.

ASCE. 2011. *Blast protection of buildings*. ASCE/SEI 59-11. Reston, VA: ASCE. These guidelines provide minimum planning, design, construction, and assessment requirements for new and existing buildings subject to the effects of accidental or malicious explosions.

ASCE. 2016. *Standard guidelines for the design, installation, and operation and maintenance of urban stormwater systems.* ASCE/EWRI Standards 45-16, 46-16, and 47-16. Reston, VA: ASCE. This set of guidelines provides for the design of urban stormwater systems, covering topics such as site analysis, system configuration, hydrology, hydraulic design, nonstructural considerations, structural design, and materials (ASCE/EWRI Standard 45-16); guidelines for the installation of urban stormwater systems and discusses subjects such as contract documents, preconstruction site inspection, construction, and inspection (ASCE/EWRI Standard 46-16); and guidelines for the operation and maintenance of urban stormwater systems, including operation and maintenance plans, water quality, periodic inspection, and maintenance (ASCE/EWRI Standard 47-16).

ASCE. 2022. *Minimum design loads for buildings and other structures*. ASCE/SEI 7-22. Reston, VA: ASCE. This update to ASCE/SEI Standard 7-16 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.

ASCE/AWWA/WEF (ASCE, American Water Works Association, and Water Environment Federation). 2004a. *Interim voluntary guidelines for designing an online contaminant monitoring system*. Reston, VA: ASCE.

ASCE/AWWA/WEF. 2004b. *Interim voluntary security guidance for wastewater/stormwater utilities*. Reston, VA: ASCE.

ASCE/AWWA/WEF. 2004c. *Interim voluntary security guidance for water utilities*. Reston, VA: ASCE.

ASCE/AWWA/WEF. 2006a. *Guidelines for the physical security of wastewater/stormwater utilities.* Reston, VA: ASCE.

ASCE/AWWA/WEF. 2006b. *Guidelines for the physical security of wastewater/stormwater utilities.* Reston, VA: ASCE.

ASIS (American Society of Industrial Security). 2012. *Protection of assets physical security*. Alexandria, VA: ASIS. This document outlines the groundwork for successful physical security projects in any situation, including the underlying concepts of security risk management, effective and efficient security practices, design principles and practices, specific tools, and techniques to satisfy protection objectives, and practical project management guidance.

ASTM. 2014. *Standard test methods for security of swinging door assemblies*. ASTM F476-14. West Conshohocken, PA: ASTM. The standard test methods covered in this document are designed to measure the capability of a swinging door assembly to restrain or delay and to frustrate the commission of "break-in" crimes. Door assemblies of various materials and types of construction covered by these test methods also include individual components such as the hinge, lock, door, jamb/strike, and jamb/wall.

ASTM. 2019. *Standard terminology relating to chain link fencing*. ASTM F552-14. West Conshohocken, PA: ASTM. This specification contains the standard terminology associated with aspects of chain-link fencing design and construction.

AWWA (American Water Works Association). 1998. *Steel water-storage tanks.* AWWA M42. Denver: AWWA. This manual provides information on the selection, design, construction, and maintenance of steel tanks for potable water storage.

AWWA. 2011. *Welded carbon steel tanks for water storage.* AWWA D100-11. Denver: AWWA. This standard provides guidance to facilitate the design, manufacture, and procurement of welded steel tanks for the storage of water. This standard does not cover all details of design and construction because of the large variety of sizes and shapes of tanks.

AWWA. 2013. *Risk and resilience management.* AWWA J100-10(R13). Denver: AWWA. The USEPA VSAT tool is intended to help identify the highest risk to mission-critical operations and find the most cost-effective measure to reduce those risks. This standard does not advocate using the tool but refers to what has been done in the past.

AWWA. 2018. *Wire- and strand-wound, circular, prestressed concrete water tanks*. AWWA D110-13(R18). Denver: AWWA. This standard details recommended practice for the design, construction, inspection, and maintenance of these types of water tanks.

AWWA. 2019. *Thermosetting fiberglass-reinforced plastic tanks*. AWWA D120-19. Denver: AWWA. This document discusses the composition, performance requirements, construction practices and workmanship, design, and methods of testing thermosetting fiberglass-reinforced plastic tanks for the storage of water and other liquids.

AWWA. 2020a. *Circular prestressed concrete water tanks with circumferential tendons*. AWWA D115-20. Denver: AWWA. This standard includes current and recommended practice for the design, construction, and field observations of circular prestressed concrete tanks using tendons for circumferential prestressing.

AWWA. 2020b. *Water wells*. AWWA A100-20. Denver: AWWA. This standard provides the minimum requirements for vertical water supply wells, including geologic/hydrologic conditions and water quality and well construction.

AWWA/ASCE. 2012. *Water treatment plant design.* 5th ed. New York: McGraw-Hill. This book is a reference for water treatment plant upgrades or new construction. Topics range from initial plans and permits through design, construction, and startup.

Echodyne. 2019. "Protecting critical infrastructure from drones." Accessed September 5, 2023. https://www.echodyne.com/media/t0gkwycg/ech_protecting-critical-infrastructure-from-drones_19s26.pdf. This white paper discusses the drone threat to critical infrastructure and the need for 3D situational awareness of the airspace using high-performance radar as part of a layered system.

Genasys, Inc. 2022. "LRAD overview and product guide." Accessed September 5, 2023. https://genasys.com/product-guides/lrad-overview-and-product-guide/. This guide provides an overview of the LRAD technology and associated benefits of using this type of device to communicate over long distances.

Hernandez, D. 2020. *Protecting against the threat of unmanned aircraft systems (UAS)*. Washington, DC: US Dept. of Homeland Security. This document outlines awareness and mitigation measures for use by federal departments and agencies to protect against malicious unmanned aircraft systems (UAS) operations.

IESNA (Illumination Engineering Society of North America). 2016. *Guideline for security lighting for people, property, and public spaces*. IESNA Publication G-1-03. New York: IESNA. This guideline covers basic security principles, illuminance requirements for several types of properties, protocols for evaluating current lighting levels for different security applications, and security survey and crime search methodology. This guideline includes exterior and interior security lighting practices for the reasonable protection of persons and property.

Jones, G. M., R. L. Sanks, G. Tchobanoglous, and B. E. Bosserman II, eds. 2005. *Pumping station design.* 3rd ed. Burlington, MA: Butterworth-Heinemann. This document provides detailed information needed to design, equip, and build efficient, reliable pumping stations that are easy to operate and maintain.

Ko, R., and K. K. Raymond Choo. 2015. *The cloud security ecosystem: Technical, legal, business and management issues*. Waltham, MA: Elsevier. This book discusses a range of cloud security topics from multidisciplinary and international perspectives, aligning technical security implementations with the most recent developments in business, legal, and international environments.

Kroll, D. J. 2006. *Securing our water supply: Protecting a vulnerable resource*. Tulsa, OK: PennWell. This book provides a detailed history of malevolent attacks against the water sector. It covers multiple types of attack methods and possible consequences. The book also references potential instrumentation to detect different types of chemical and biological attacks.

Mays, L. R., ed. 2000. *Water distribution systems handbook*. New York: McGraw-Hill. This handbook provides material to design, analyze, operate, maintain, and rehabilitate water distribution systems. Topics include hydraulic design for pipelines and tanks to water quality issues, computer models, and rehabilitation/replacement information.

NFPA (National Fire Protection Association). 2017. *National electrical code*. NFPA 70. Quincy, MA: NFPA. This code describes the safe installation and use of electrical equipment by consumers.

NFPA. 2018. *Life safety code*. NFPA 101. Quincy, MA: NFPA. This code addresses those egress features necessary to minimize danger to life from fire and smoke, crowd pressures, and movement of individuals and groups. It provides minimum criteria for the design of egress facilities to permit prompt

escape of occupants from buildings or, where desirable, into safe areas within buildings.

Nilsson, F., and AXIS Communication. 2017. *Intelligent network video: Understanding modern video surveillance systems*. Boca Raton, FL: CRC Press. This book examines networked surveillance video solutions. It provides the latest details on industry hardware, software, and networking capabilities of the latest cameras and DVRs.

Teledyne FLIR. 2021. *Applying ground-based security radar to perimeter systems. White paper*. Wilsonville, OR: Teledyne FLIR. This white paper discusses the technology, application, and advantages of ground radar systems in physical security applications.

US Code. 2009. *42 U.S.C. §300(i)(1)*. Washington, DC: Office of the Law Revision Counsel. This is US Code Title 42, Section 300i-1, *Tampering with Public Water Systems*.

US Congress. 2018. "John S. McCain national defense authorization act for fiscal year 2019." Accessed August 23, 2023. https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

US DOD (US Department of Defense). 2010a. *Design and O&M: Mass notification systems*. UFC 4-021-01. Washington, DC: DOD. The UFC system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.

US DOD. 2010b. *Selection and application of vehicle barriers*. UFC 4-022-02. Washington, DC: DOD. The UFC system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.

US DOD. 2013. *Security fences and gates*. UFC 4-022-03. Washington, DC: DOD. The UFC system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.

US DOD. 2017. *Entry control facilities access control points*. UFC 4-022-01. Washington, DC: DOD. The UFC system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.

US DOD. 2019. *Electronic security systems*. UFC 4-021-02. Washington, DC: DOD. The UFC system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.

US DOD. 2022. *Minimum antiterrorism standards for buildings*. UFC 4-010-01. Washington, DC: DOD. The UFC system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.

USEPA. 2021. *Baseline information on malevolent acts for community water systems version 2.0. Office of water (MC 140)*. EPA 817-F-21-004. Washington, DC: USEPA. This document is intended to help utilities identify malevolent acts and provides an estimation of threat likelihood for malevolent acts identified in the AWWA J100-10 Reference Threats.

US GSA (General Services Administration). 2005. *Facilities standards for the public buildings service*. Washington, DC: GSA. These design standards and criteria are to be used in the programming, design, and documentation of GSA buildings.

Wallace, D. W., and L. Foster. 2021. *A logical basis for cumulative defense strategy and the mathematical analysis of defense strategy and countermeasures (MADSC)*. Lafayette, CO: Critical Security Research and Analysis Center (CSRAC). This white paper describes how the lack of available intelligence or historical frequency data on malevolent attacks has caused an inadvertent gap in physical security for the water sector. A new methodology is proposed outlining a new risk model to help accurately guide the application and justification of physical security countermeasures.

Wallace, D. W., D. Lewin, K. Schartau, L. Foster, and C. G. Keyes Jr. 2024. "Empirical risk analysis methodology for adversarial threats against critical infrastructure." *J. Infrastruct. Syst.* 30 (1): 04023036. https://doi.org/10.1061/JITSE4.ISENG-2291. This journal paper details three dilemmas caused by existing water risk resilience assessments and standards. It also details an effective new risk model and the high-level theory behind the Foster–Wallace formula.

WEF (Water Environment Federation). 1992. *Design and construction of urban stormwater management, manual of practice no. FD-20*. Alexandria, VA: WEF. This document provides design and construction best practices for urban stormwater management.

WEF. 1993. *Design of wastewater and stormwater pumping stations, manual of practice no. FD-4*. Alexandria, VA: WEF. This manual focuses on the design of wastewater and stormwater pumping stations.

WEF. 1999. *Wastewater collection systems management, manual of practice no. 7*. 5th ed. Alexandria, VA: WEF. This document is a reference for the operation and maintenance of a wastewater collection system.

WEF. 2005. *Operation of municipal wastewater treatment plants, manual of practice no. 11*. 6th ed. Alexandria, VA: WEF. This three-volume manual of practice covers the operation of municipal wastewater treatment plants. Volume I, "Management and Support Systems," covers plant management, support systems, plant operations, safety and health, and chemical application systems. Volume II, "Liquid Processes," addresses characterization and sampling of municipal wastewater, select biological processes, and other related topics. Volume III, "Solids Processes," includes sludge thickening, aerobic and anaerobic digestion, sludge and lime stabilization, disposal of biosolids, and related topics.

WEF. 2007. *Gravity sanitary sewer design and construction, manual of practice no. FD-5*. Alexandria, VA: WEF. This manual is the second revision of the relevant portions of the ASCE/WPCF Manual of Practice No. 37, *Design and Construction of Sanitary and Storm Sewers*, and presents the current practice in the field of sanitary sewer design and construction. Its intended audience is design professionals knowledgeable in the areas of gravity sewers.

WEF. 2010. *Design of municipal wastewater treatment plants, manual of practice no. 8*. 5th ed. Alexandria, VA: WEF. This is the industry standard for wastewater design. This is also ASCE MOP 76.

WSWG (Water Security Working Group). 2005. *Recommendations of the national drinking water advisory council to the U.S. Environmental Protection Agency on water security practices, incentives, and measures*. Washington, DC: WSWG. 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.

Wyss, G. D., J. F. Flem, J. L. Darby, and K. Dunphy-Guzman, et al. 2011. *A risk-informed method for enterprise security*. Albuquerque, NM: Sandia National Laboratories. This document details an advanced equation that does not rely on threat likelihood to evaluate risk.

This page intentionally left blank

INDEX

Page numbers followed by *f* or *t* indicate figures or tables.

This page intentionally left blank

ATTACHMENT E

SJWC INDEX 5284-APPENDIX C

AWWA G430-14 STANDARD ANALYSIS

AWWA G430-14 REQUIREMENTS DESCRIPTION	Camera System	Head End	Intrusion Detection System	Access Control	Fencing, Gates, & Barriers	Plan Policy and Protocol	Training and Exercises	Assessments	Guard Service	Systems Monitoring Maintenance and Testing	Background Checks	Threat Monitoring	Staffing
Section 4.1 Explicit Commitment to Security													
4.1.1 Explicit and visible commitment of senior leadership to security. **The utility shall establish an explicit, visible, easily communicated, enterprise-wide commitment to security. This shall be represented by the development of a security plan, by policies, and by other documents that make security a part of daily operations visible to employees and customers.**						Required							
4.1.1.1 Periodic review and update of security plan, policies, or documents. The utility **shall establish and maintain a schedule for periodic review of its security plan, policies, and documents, and update them as needed.**						Required							
Section 4.2 Security Culture													
4.2.1 Promote security awareness throughout the utility. **The utility shall promote a culture whereby every person understands, appreciates, and contributes to enhanced security.**						Supporting	Supporting						
4.2.1.1 Employee reports and suggestions. **The utility shall establish a process for employees to report security violations or concerns and to make suggestions for improvement.**						Required	Supporting						
4.2.1.1 Employee training. **The utility shall train employees and other responsible parties in security awareness, individual responsibility, and appropriate responses.**						Supporting	Required						
4.2.1.2 Incorporating security into job descriptions. **The utility shall include security in job performance evaluations and rate employees, including top management, on their performance.**						Supporting							
4.2.1.3 Measure security activities and progress. **The utility shall establish a means of measuring security activity, establish goals for improvement, and monitor progress.** The utility should review the recommended performance measures under the Water SSP of the NIPP, and consider them as a standardized mechanism for measurement and reporting that may supplement the requirements of this standard. The utility should also consider using the self-assessment questions included therein as a guide for improvement.						Required							
4.2.1.4 Visible identification. **The utility shall establish a means of visible identification of employees and others authorized to access utility facilities, and ensure every person routinely complies.**				Required		Required							
4.2.2 Reward employees for appropriate security activities. **The utility shall have a means of rewarding appropriate security awareness and response by employees and others.**						Supporting							
Section 4.3 Defined Security Roles and Employee Expectations													
4.3.1 Identify managers and employees who are responsible for security. **The utility shall identify managers and employees responsible for creating, maintain- ing, and implementing the security plan; for performing and maintaining the vulnerability or risk assessment; and for providing security leadership. Other security-related roles and responsibilities include security program management, physical intrusion and contamination detection, and incident command roles during emergency response and recovery.** Additional roles and responsibilities should be identified on a utility-specific basis as appropriate.						Required	Supporting						
4.3.2 Establish security expectations for staff. **The utility shall identify and disseminate security expectations for staff and periodically review performance.**						Required							
Section 4.4 Up-to-Date Assessment of Risk													
4.4.1 Perform a risk assessment. **The utility shall perform a risk assessment. The utility's risk assessment may use publicly or commercially available tools, consistent with ANSI/AWWA-J100, that allow the assessment to be replicated and based on the following steps:**						Supporting		Required				Required	
1. Asset characterization								Required					
2. Threat characterization								Required					
3. Consequence analysis								Required					
4. Vulnerability analysis								Required					
5. Threat likelihood analysis								Required					
6. Risk/resilience likelihood								Required					
7. Risk/resilience analysis								Required					
4.4.2 Review and Update. **The utility shall review and update its risk assessment as new hazards and threats emerge, when facilities are constructed or removed from service, and when other changes occur that significantly affect the results of the risk assessment.**						Supporting		Required				Required	
4.4.2.1 Periodic review. **The utility shall establish and maintain a schedule for periodic review and update of its risk assessment, based on the utility- specific circumstances. The schedule for review shall not exceed five years but can be more frequent based on operational changes or other incidents that warrant further review.**						Supporting		Required				Supporting	
4.4.2 Review and update. **The utility shall review and update its risk assessment as new hazards and threats emerge, when facilities are constructed or removed from service, and when other changes occur that significantly affect the results of the risk assessment.**						Supporting		Required				Required	
4.4.2.1 Periodic review. **The utility shall establish and maintain a schedule for periodic review and update of its risk assessment, based on the utility-specific circumstances. The schedule for review shall not exceed five years but can be more frequent based on operational changes or other incidents that warrant further review.**						Supporting		Required				Supporting	
Section 4.5 Resources Dedicated to Security and Security Implementation Priorities													
4.5.1 Sustain focus on security. **The utility shall sustain a focus on security by maintaining security as a current priority.**						Required							
4.5.1.1 Maintain focus. **Executives and line managers shall maintain a focus on security throughout the years by doing one or more of the following items, or a defined alternative:**						Required							
• Include security in periodic progress reports to the governing body						Required							
• Make security a standing item on executive management agendas						Required							
• Make security a routine item in manager or supervisor meetings with employees or other authorized persons						Required							Supporting
4.5.1.2 Resources. **The utility shall invest staff time and resources in security by including security considerations in budgets for personnel and training or, if appropriate, by explicitly assigning security responsibilities to existing staff and budgeting accordingly.**						Required	Supporting						Supporting
4.5.1.3 Exercises. **The utility shall include security exercises in operational planning and identify associated training costs in budgets.**						Required	Supporting						
4.5.2 Identify security priorities. **The utility shall establish a security improvement plan that identifies security priorities based on its risk assessment (see Sec. 4.4).**						Required		Required					

AWWA G430-14 REQUIREMENTS DESCRIPTION	Camera System	Head End	Intrusion Detection System	Access Control	Fencing, Gates, & Barriers	Plan Policy and Protocol	Training and Exercises	Assessments	Guard Service	Systems Monitoring Maintenance and Testing	Background Checks	Threat Monitoring	Staffing
4.5.2.1 Integrate security plan. **The utility shall integrate the security improvement plan with other operational plans and investments and shall establish the appropriate relationship of security priorities based on the utility's vulnerability assessment in context with other organizational priorities.**						Required		Required					
4.5.2.2 Identify resources required for the security plan. **The utility shall identify and commit resources dedicated to security programs and planned security improvements. Based on the relationship with other organizational priorities, the utility shall identify and plan for the resources required to maintain the security program and make necessary improvements.**	Supporting	Supporting	Supporting	Supporting	Supporting	Required		Required	Supporting				Supporting
Section 4.6 Access Control and Intrusion Detection													
4.6.1 Identify utility assets requiring access control. **Through the risk assessment or other means, the utility shall identify assets or facilities that require con- trolled access based on criticality to maintain normal operations (identified critical assets).**				Required	Required			Required					
4.6.2 Establish and maintain physical control of access to identified critical assets. **The utility shall establish and maintain a means of physically controlling access to identified critical assets**. Examples of physical access controls include the following and can be used individually or in combination:				Required	Required	Supporting			Supporting	Required			
• Substantial buildings with intrusion prevention devices on windows and access pomts			Required	Supporting						Required			
• Fences					Required					Required			
• Barriers					Required					Required			
• Locked gates, hatches, and doors			Supporting	Supporting	Required					Required			
• Monitored intrusion alarms		Required	Required						Supporting	Required			
• Tamper-resistant devices at key distribution or collection points				Required	Required								
4.6.3 Implement annual inspections of identified critical assets. **The utility shall implement and maintain annual inspections to assure that security features are adequate and functioning, and to identify if any corrective work is necessary to maintain access control or other security features.**						Required	Supporting	Required					
4.6.4 Establish and maintain a means of detecting and assessing intrusion. **The utility shall establish and maintain a means of detecting and assessing intrusion into identified critical assets by unauthorized persons in a manner that is timely and enables the utility to respond effectively.** Monitoring for physical intrusion can include physical and procedural improvements. Examples of physical improvements include installing detection devices such as motion detectors and intrusion alarms, or improved assessment tools such as well-lighted facility perimeters, or monitoring with closed-circuit TV (CCTV). Procedural improvements include the use of neighborhood watches, regular employee rounds, or arrangements with the local police or fire department to help identify and report unusual activity.	Required	Required	Required	Required	Required				Supporting	Required			
4.6.5 Establish and maintain procedures to control personnel access to identi-fied critical assets. **The utility shall establish and maintain procedural controls to limit access to identified critical assets to authorized persons only.** Examples of procedural access controls include the following and can be used individually or in combination:			Required	Required		Supporting	Supporting			Required			
• Inventory and control keys						Required	Supporting						
• Develop procedure that limits access rights to employees to maximum extent possible						Required	Supporting			Supporting			
• Develop hierarchical key and/or access card system to limit access to extent possible						Required	Supporting			Supporting			
• Change access codes regularly				Supporting		Required	Supporting			Supporting			
• Require security passes for access				Required		Required	Supporting		Supporting				
• Establish a security presence at access points				Required		Required	Supporting		Supporting				
• Require visitors to have scheduled appointments, and/or have a protocol to address unscheduled visitors				Supporting		Required	Supporting						
• Require employees and other authorized persons to display identification at all times when on-site, if appropriate						Required	Required						
• Require visitors to sign in and display identification at all times when on-site				Required		Required	Required						
• Implement chemical delivery and testing procedures including chain-of-custody control or tamper-evident packaging requirements						Required	Supporting						
• Limit delivery hours						Required	Supporting		Supporting				
• Check deliveries to ascertain the nature of the material				Supporting		Required	Supporting		Supporting				
4.6.6 Establish and maintain a means of restricting authorization for access. **The utility shall establish and maintain a means of restricting unescorted access to identified critical assets.**				Required		Required	Supporting		Supporting	Supporting			
4.6.6.1 Background checks. **Where legally permissible and appropri-ate, the utility shall institute a system of background checks on employees, con- tractors, temporary workers, or any other person authorized to access identified assets without an escort.** The level or complexity of background checks used should be commensurate with the level of access and the privileges granted to the person. Other benefits of background checks, depending on the level employed, may include verifying identity, establishing citizenship, determining previous criminal activity, and determining work eligibility.						Required	Supporting				Required	Supporting	
4.6.6.2 Other means of identity verification. **When background checks are not permitted or appropriate, the utility shall establish a defined alternative method of verifying identity and granting access rights and privileges to a person seeking authorization.**						Required	Supporting				Required	Supporting	
4.6.7 Establish a protocol for employees or others who have been terminated, have resigned, or have had a relevant change of status. **The utility shall establish and maintain a protocol to recover keys, revise passwords, and take other appropriate actions immediately on termination, resignation or re-assignment of an employee or the relevant change of status of other personnel who have access to high-risk assets.** Other personnel may include vendors, consultants, contractors, public officials, or others who had been granted appropriate access and are no longer performing a relevant function.						Required	Supporting					Supporting	
4.6.8 Testing. **The utility shall test physical and procedural access controls routinely to ensure performance. The tests shall be conducted annually, or more frequently if required by law or regulation.**		Supporting	Supporting	Supporting		Required	Required			Supporting			
Section 4.7 Contamination Detection, Monitoring, and Surveillance													

AWWA G430-14 REQUIREMENTS DESCRIPTION	Camera System	Head End	Intrusion Detection System	Access Control	Fencing, Gates, & Barriers	Plan Policy and Protocol	Training and Exercises	Assessments	Guard Service	Systems Monitoring Maintenance and Testing	Background Checks	Threat Monitoring	Staffing
4.7.1 Surveillance and response for chemical, biological, or radiological contami-nation. **The utility shall develop and implement a surveillance and response system.** A surveillance and response system provides a proactive approach to manag-ing threats that uses monitoring technologies/strategies and enhanced surveillance activities to collect, integrate, analyze, and communicate information. However, it should not be merely a collection of monitors and equipment placed throughout a water distribution system to alert of intrusion or contamination, but rather should be an exercise in information acquisition and management. Different information streams are captured, managed, analyzed, and interpreted to recognize potential contamination incidents in time to respond effectively. While the surveillance and response system should be designed by the drinking water utility, some data sources may be outside of the utility, and in this case, cooperation with partners would likely be important to the success of a surveillance and response system. The recommended components of a surveillance and response system are briefly described as follows:	Required	Required	Required	Required	Required	Required	Required		Supporting	Supporting			
• Enhanced security monitoring includes the equipment and procedures that detect and respond to security breaches at distribution system facilities.	Required	Required	Required	Required	Required	Required	Required		Supporting	Supporting			
4.7.2 Monitoring or surveillance of indicators of contamination. Although typical water quality parameters (surrogate parameters) may not be a direct indication of chemical, biological, or radiological contamination, the utility may find that monitoring surrogate parameter concentrations or trends is useful and appropriate in its individual circumstance. Recognizing that surrogate parameter changes may be difficult to interpret from a security perspective, the utility should review and consider any physical security monitoring anomalies, such as intrusion alarms, CCTV records, and so on, in its evaluation. Examples of surrogate parameters being utilized by utilities include the following:	Required	Required	Required	Required	Required	Required	Required		Supporting	Supporting			
4.7.3 Laboratory testing for contaminants. **The utility shall routinely sample and monitor the water or wastewater system as required by law or regulation, and shall include additional test parameters or elevated sampling frequencies if appropriate to a specific security concern or threat notification.** The utility should consider identifying and prequalifying laboratories that have the necessary capabilities.						Required	Supporting			Required			
4.7.4 Communication with customers and public health authorities as a means of identifying contamination. **The utility shall monitor customer complaints and initiate or improve communications with local public health authorities or networks.**						Required	Supporting			Required			
4.7.4.1 Documentation of complaints. **The utility shall establish a means to record and analyze customer complaints and evaluate them as indicators of possible system contamination**. This system should include communications with customer communities that receive bulk water deliveries, if appropriate.						Required	Supporting						
4.7.4.2 Communication. **The utility shall establish and maintain two-way communications and relationships with local public health authorities and health providers to expedite the potential identification of public health anomalies that may be indicators of system contamination.**						Required	Supporting						
4.7.5 Adjacent utilities. **The utility shall establish and maintain two-way communications with adjacent utility systems to identify any contamination. In the case of a water utility, this may be an upstream water or wastewater utility.** In the case of a wastewater utility, this may be downstream users or others that assess the receiving stream quality.						Required	Supporting						
4.7.6 Incident detection and response. **The utility shall establish written procedures for, at a minimum, the following key components of a surveillance and response system: (1) the criteria that will be used to identify a potential contamina- tion event and trigger an investigation, (2) the criteria that will be used to declare that a contamination incident has occurred, and (3) the response protocol for a contamination incident. This response protocol should be a part of the utility's emergency response plan** (see Sec. 4.11).						Required	Supporting						
Section 4.8 Information Protection and Continuity													
4.8.1 Define security-sensitive systems and information. For most systems, information technology (IT), Process Control Systems, and SCADA systems are essential to the efficient and continuous operations of a utility. **The utility shall identify critical IT, Process Control Systems, or SCADA systems as security-sensitive. The utility shall also identify other security-sensitive information. This information review shall consider facility maps and other geographic sources on utility operations, security plans, vulnerability assessments, or other technical details that could aid an adversary in the planning or execution of an attack.** For additional information and useful tools for critical cyber system identifica-tion and protection, the user is directed to *Appendix A, Section A.7-AWWA Process Control System Security Guidance for the Water Sector, and Section A.8-Cyber Security Evaluation Tool (CSET).*						Required	Supporting	Required					
4.8.1.1 Secure information. **The utility shall evaluate the information it shares with vendors, bidders, or the public (e.g., facility tours, brochures, or internet access). Where appropriate and practicable, security-sensitive information shall be removed or controlled.**						Required	Supporting						
4.8.1.2 Regulations. **The utility shall consider any applicable freedom of information or Sunshine Act provisions with which it must comply, to understand and abide by limitations on controlling information.**						Required	Supporting						
4.8.2.1 Restricting access. **The utility shall identify and implement steps necessary to control access to critical IT, Process Control Systems, and SCADA systems to only authorized persons conducting official utility business. Physical hardening and procedural controls shall be considered and implemented.** The following are examples of procedural controls:	Required	Required	Required	Required	Required	Required	Supporting		Supporting	Required	Supporting	Supporting	
• Restricting access to data networks	Required	Required	Required	Required	Required	Required	Supporting			Required			
• Implementing policies to ensure that IT contractors or their produces will not negatively affect IT systems	Required	Required	Required	Required	Required	Required	Supporting			Required			
• Ensuring security at each location of SCADA components	Required	Required	Required	Required	Required	Required	Supporting			Required			
4.8.4 Detect unauthorized access. **The utility shall establish and maintain the means to detect unauthorized access or intrusion to IT, Process Control Systems, or SCADA systems, or to security-sensitive information, and the means to respond in an appropriate and timely manner.** For additional information on intrusion detection systems and defense-in-depth strategies, *see appendix A, Section A.7.*	Required	Required	Required	Required	Required	Required	Supporting		Supporting	Required	Supporting	Supporting	
4.8.5.1 Critical information. **The utility shall identify critical information and ensure its preservation and accessibility during emergency response and recovery. Off-site backup of critical data should be considered for preservation and accessibility.**						Required	Supporting						
4.8.5.2 Critical communications. **The utility shall identify critical internal and external communications and ensure their functionality during emergency response and recovery.**						Required	Supporting			Supporting			
Section 4.9 Design and Construction													
4.9.1 Incorporate security objectives into utility design and construction stan-dards. **Consistent with the recommendations of the vulnerability or risk assessment where applicable, the utility shall incorporate its security objectives into the design of infrastructure repairs or replacements, or the acquisition or construction of new assets.**						Required		Required					
4.9.1.1 Physical hardening of identified critical assets. **The utility shall include physical hardening in the repair/replacement of identified critical assets, or in the design and construction of new assets.** Physical hardening is intended to protect or help mitigate physical damage, service disruption, or other serious con- sequences of an attack by making the facility harder to attack or by reducing the effect an attack may have. Following are examples of physical hardening:					Required	Required		Required					

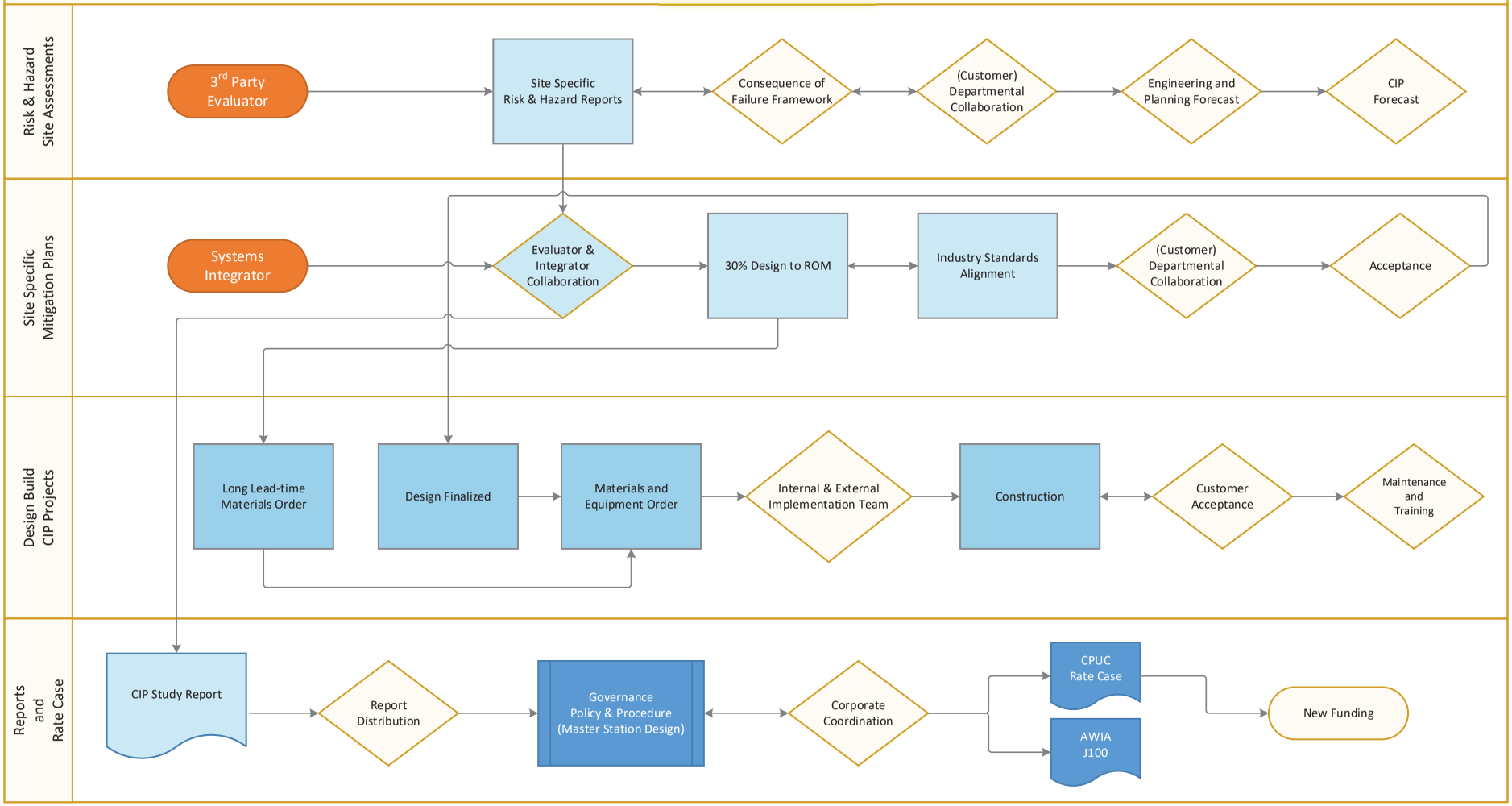
AWWA G430-14 REQUIREMENTS DESCRIPTION	Camera System	Head End	Intrusion Detection System	Access Control	Fencing, Gates, & Barriers	Plan Policy and Protocol	Training and Exercises	Assessments	Guard Service	Systems Monitoring Maintenance and Testing	Background Checks	Threat Monitoring	Staffing
• Location of critical assets within a facility						Required		Required					
• Use of substantial building materials						Required		Required					
• Designing in inherent redundancy for critical services						Required		Required					
Design choices should also consider the ability to ensure continuity of operations and rapid recovery in the event of an attack, natural disaster, or other event.						Required	Required	Required					
4.9.1.2 Adoption of security risk technologies or approaches . **The utility shall consider the adoption of security technologies or approaches that have the demonstrated capability of reducing or mitigating the consequences of an attack, natural disaster, or other event when making design or technology choices.** Examples of such technologies and approaches include Crime Prevention Through Environmental Design (CPTED), increased redundancy of critical components, increased interconnections with adjacent utilities, and increased agreements for shared storage of spare parts and equipment.	Required	Required	Required	Required	Required	Required		Required		Required			
Section 4.10 Threat-Level-Based Protocols													
4.10.1 Monitor available threat-level information. **The utility shall establish an appropriate means to stay apprised of changes in threat levels. Sources of information may include the US Department of Homeland Security (DHS), local police or FBI office, WaterISAC, InfraGard, or other credible sources.** The utility should research and establish communications with networks and information sources appropriate to its security environment.										Required		Required	Required
4.10.2 Escalate security procedures in response to relevant threats. **The utility shall establish a procedure to escalate security operations in the event of a relevent increase in the threat level or a significant local event.**						Required	Required	Supporting				Required	Required
Section 4.11 Emergency Response and Recovery Plans and Business Continuity Plan													
4.11.1 Incorporate security into emergency response and recovery plans, business continuity plans, and operations.						Required	Supporting			Supporting			
4.11.1.1 Update plans . **The utility shall revise its emergency response and recovery plans and business continuity plans as necessary to incorporate security considerations into the plans.** Additional guidance is provided in *ANSI/AWWA G440 and Business Continuity Planning for Water Utilities* (Water RF 2008) .*						Required	Supporting						
4.11.1.2 Emergency response . **The utility shall comply with the National Incident Management System (NIMS) guidelines, and use Incident Command System (ICS) protocol for emergency response.**						Required	Required						
4.11.2 Test emergency response and recovery plans and business continuity plans regularly. **The utility shall establish and maintain a schedule for testing its emergency response and recovery plans and business continuity plans.** Testing may include training, tabletop exercises or drills, or real-time simulated responses.						Required	Required						
4.11.3 Update emergency response and recovery plans and business continuity plans as necessary.						Required	Required						
4.11.3.1 Review and update . **The utility shall perform a timely review and update its emergency response and recovery plans and business continuity plans as necessary to correct identified deficiencies after exercises or actual implementation (lessons learned) in accordance with ANSI/AWWA G440.**						Required	Supporting	Supporting					
4.11.3.2 Routine reviews . **The utility shall perform a timely review and update of its emergency response and recovery plans and business continuity plans routinely and as necessary to reflect relevant changes in potential threats, physical infrastructure, utility operations, critical interdependencies, or response protocols in partner organizations. In no event shall the interval exceed five years, but the review and update can be more frequent if required by law or regulation.**						Required	Supporting	Supporting				Required	
4.11.4 Contact list. **The utility shall establish, maintain current, and dis-tribute a list of contacts to include key employees and key contacts for critical cus-tomers and support organizations. This list shall include names, phone numbers, and other information necessary to establish contact with those persons or designated alternates during an emergency.**						Required							Required
4.11.5 Response to contamination threat. **The emergency plan shall have a procedure for responding to potential contamination events or threats, which provides reporting out, field verification, credibility assessments, site sampling, lab qualification, lab analysis, and public notification.**						Required	Required	Required		Supporting			
4.11.6 Protection of public health. **The utility must be prepared to consider contamination evidence carefully and make public health decisions with incom- plete data and analysis.**						Required	Required			Supporting			
Section 4.12 Internal and External Communications													
4.12.1 Establish and maintain strategies for regular and ongoing communications with employees. **The utility shall establish and maintain strategies for effective communications with employees about security issues.** These strategies should be designed to maintain security awareness, to motivate staff to take security seriously, to allow staff to notify security personnel or others about security concerns or suspicious events or activities, to promote employee safety during an event, and to enable effective employee participation during an event. **The utility shall evaluate the need and means for providing backup systems that will maintain commu-nications with employees during an emergency response and recovery.**						Required				Supporting			
4.12.2 Establish and maintain strategies for regular and ongoing relationships and communications with response organizations. **The utility shall establish and maintain strategies for effective relationships and communications with response organizations. The utility's strategies should focus on ensuring clarity and reliability of information during an emergency. The utility shall evaluate the need and means for providing backup systems that will maintain communications with agencies such as police, fire, and other first responders during an emergency response and recovery.**						Required				Supporting			
4.12.3 Establish strategies for regular and ongoing communications with customers. **The utility shall establish strategies for effective communications with customers prior to any emergency. Communications strategies should especially consider the most effective way to reach customers with information, both in terms of delivery and source, and ways to get information from customers about unusual events or suspicious activities.** The utility's strategies should consider key messages, which person is equipped and trusted to deliver the messages, and the need for consistency, especially during an emergency.						Required				Supporting			
4.12.4 Establish strategies for regular and ongoing communications with regulatory agencies. **The utility shall establish strategies for effective communications with relevant regulatory agencies.** Communications strategies should consider timely two-way communications in the event of an actual incident or threat.						Required				Supporting			
Section 4.13 Partnerships													
4.13.1.1 Identify key partnerships. **The utility shall identify key agencies that are essential to emergency response and recovery and establish and maintain collaborative partnerships with these agencies.** Customer community agencies such as police and fire, managers of critical interdependent infrastructure such as power companies, first-responder agencies, and adjacent utilities are typically included as key agencies.						Required	Supporting						
4.13.1.2 Establish collaborative partnerships . **The utility shall establish collaborative partnerships with key agencies as appropriate to ensure cooperation and effective coordination during emergency response and recovery.**						Required	Supporting						

ATTACHMENT F

PHYSICAL SECURITY CIP PROCESS FLOW CHART

Physical Security CIP Process Flow

San Jose Water Company



ATTACHMENT G

PHYSICAL SECURITY PRESENTATION FIELD TOUR

CONFIDENTIAL VERSION

DECLARATION OF JOHN B. TANG
REGARDING THE CONFIDENTIALITY OF CERTAIN DATA
ACCOMPANYING SAN JOSE WATER COMPANY'S
REBUTTAL TO CAL ADVOCATES GENERAL RATE CASE 2024

I, John B. Tang, declare and state:

1. I am Vice President – Regulatory Affairs & Government Relations at San Jose Water Company. I am an officer of San Jose Water Company (SJWC).

2. I have also reviewed Exhibit G: 2024-2026 Capital Improvement Project justification and Appendices 1. This was reviewed specific to Index #5284 which includes a detailed list of all the different types of Safety and Security Plans proposed for SJWC. The cost breakup between Operating and Expense category has also been detailed. Index#5284 justification outlines the actual security threats to the entire SJWC system with specific mention of areas of threat and ways to mitigate it. Since this justification is very specific it has been classified as Confidential. If this report is made public, there can be compromises in securing all of SJWC's assets thereby impacting employee and customer safety. It is the position of SJWC that confidential treatment of the referenced information is warranted pursuant to the statutory and regulatory authorities specified in Paragraph 6 of this Declaration.

3. I have personal knowledge of the facts and representations of fact stated in this Declaration and, if called upon to testify, could and would do so competently, except such facts or representations as are stated to be based upon information and belief, and as to those matters, I believe them to be true.

4. Listed below are references to the information and data for which San Jose Water Company is seeking confidentiality protection and the basis for San Jose Water Company's confidentiality request.

Location of Confidential Information	Pages (if available)	Description of Information that is Confidential	Basis for Confidentiality Claim
SJWC Rebuttal Testimony to Cal Advocates -Mark Hatcher on Physical Security Capital Improvement Project and Expenses	Attachment G	This document contains confidential utility systems information, including information related to safety and security projects from which specific system vulnerabilities can be determined. These sections constitute critical infrastructure information (CII) that is not customarily in the public domain, relating to the security of critical infrastructure or protected systems. The disclosure of such information presents a public safety threat as it would expose vulnerabilities San Jose Water's water distribution infrastructure, thereby endangering public safety. The public interest served by not disclosing the information in this document clearly outweighs the public interest served by disclosure of the information contained. These documents also qualify for confidentiality under the public interest balancing test. Disclosure of the information at issue here increases the odds of an attack on San Jose Water's infrastructure. It also increases the odds that any attack would be successful. Any	Cal Govt. Code §§7927.300, 7927.705, 7929.205, 7922.000; 6 U.S.C. §131(3), 133(a)(1)(E); 6 C.F.R. §§29.2, 29.8; and Pub. Util. Code §583

		attack, especially a successful one, on San Jose Water's infrastructure runs a high likelihood of disrupting service to San Jose Water's customers. Moreover, any attack would likely lead to an increase in San Jose Water's customers' rates based on the costs of responding to, and then alleviating the effects, of an attack. The interests of any member of the public knowing the specific details of San Jose Water's critical infrastructure are minimal, if not non-existent. As such, based on the risk of disruption of service and increased costs, the public interest in nondisclosures clearly outweighs any public interest in disclosure. This information should not be customarily in the public domain, relating to the nature of critical infrastructure or protected systems. The public interest served by not disclosing the information in this document clearly outweighs the public interest served by disclosure of the information contained.	

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on May 31, 2024, at San Jose, California.

John B. Tang