Chapter 15 Physical Security

Appendices

List of Figures

Chapter 15 PHYSICAL SECURITY

This chapter of the Design Standards and Guidelines (DSG) describes methods and strategies for physical security at Seattle Public Utilities (SPU) properties. The primary audience for this chapter is both project coordinators and internal SPU asset owners/operators. DSG standards are shown as underlined text.

By protecting the public's drinking water and wastewater, SPU ultimately protects the public's health. Presidential Policy Directive 21 identifies water and wastewater as one of the sixteen critical infrastructure sectors in the nation. SPU is responsible for maintaining and protecting drinking water, solid waste, drainage, and wastewater. This complex landscape of infrastructure requires that security measures be implemented according to the specific needs of existing infrastructure, facilities, and operating environments.

15.1 KEY TERMS

The abbreviations and definitions given here follow either common American usage or regulatory guidance.

15.1.1 Abbreviations

Abbreviation	Term
AWWA	American Water Works Association
CCTV	closed-circuit television
CBR	chemical, biological, or radiological
CPTED	Crime Prevention Through Environmental Design
DBT	design basis threat
DBU	database unit
DHS	Department of Homeland Security
DVR	digital video recorder
FEMA	Federal Emergency Management Agency
ft	feet
HID	HID Global
IED	improvised explosive device
IT	information technology
LED	light emitting diode
ORC	Operations Response Center

Abbreviation	Term
PPS	physical protection system
PTE	potential threat elements
PTZ	pan-tilt-zoom
PVC	polyvinyl chloride
SCADA	Supervisory Control and Data Acquisition
SMC	Seattle Municipal Code
SOP	standard operating procedure
SPU	Seattle Public Utilities
UPS	uninterruptible power supply

15.1.2 Definitions

Term	Definition
All-inclusive integrated security strategy	SPU's guiding standards for developing a security strategy that accounts for security features early on in a project's life cycle and considers the specific security needs of each facility and infrastructure.
AMAG system	A physical security system developed by evaluating how a facility or infrastructure may be targeted and establishing proper countermeasures, including technology and threat and risk assessments, to prepare, deter, detect, delay, and respond.
Asset	A property, facility, infrastructure, or construction project under the authority and protection of SPU.
DBTs	Vulnerabilities identified based on physical characteristics and projected SOPs for an asset.
CPTED	Security strategies that rely on altering the physical and environmental design to deter criminal behavior by influencing the decisions of those posing the threat before they commit a criminal act. Implementing CPTED barriers is cost effective and reduces criminal opportunity.
Risk assessment	Assessing the risk to a facility or infrastructure as the probability of an undesirable event transpiring, the capacity to address a potential loss, and the likelihood of the event's occurrence.
Threat assessment	Assessing the potential for natural and human threats facing an asset. Threats may include natural disasters, extreme weather conditions, malicious acts, ranging from vandalism to terrorism.

15.2 GENERAL INFORMATION

This chapter provides a comprehensive preliminary guideline for addressing security concerns for SPU assets, including properties, infrastructure, facilities, and construction projects. This encompasses security measures for designing new facilities or redesigning physical security measures for existing facilities. SPU's Security Department adheres to multiple physical

protection standards, including industry best practices and recommendations from the American Water Works Association (AWWA), Department of Homeland Security (DHS), and Federal Emergency Management Agency (FEMA). SPU's minimum physical security standards allow flexibility in designs, approaches, and tactics based on each asset's operating conditions. After conducting a full comprehensive risk assessment (see DSG section 15.3.2) or an individual consequence threat assessment, the Security Department can recommend cost-effective risk mitigation methods.

15.2.1 Asset Protection

With 1,823 miles of water pipeline and 31 billion gallons of water supply storage at two mountain reservoirs, SPU is responsible for protecting a large network of the public water supply and its infrastructure. SPU has various pump stations, chemical buildings, and solid waste transfer stations that all require security. Protecting SPU assets is imperative to keeping SPU's promise to community partnerships and allows a focus on what is important to SPU's residential and business customers. Securing SPU assets includes the protection of public health, safety, and confidence.

The water sector is a lifeline sector, where significant interruption can have a catastrophic effect on the public's health, environment, and economy. Risks to the protection of assets include malicious acts such as crime or terrorism, non-malicious acts such as accidents or negligence, and natural disasters such as storms or earthquakes. SPU's objective is to protect its assets, and thus the public, against potential risks by implementing sustainable efforts to reduce risk while accounting for the cost and benefits of security investments. A Security Department representative can conduct a risk assessment (see DSG section 15.3.2) to identify vulnerabilities in assets critical to meeting SPU's mission to provide efficient and innovative utility services.

15.2.2 Intrusion Prevention

Intrusion prevention relies on physical and procedural access control measures to restrict access to SPU infrastructure. Establishing security measures prepares for, deters, detects, delays, and responds to unauthorized intrusions to SPU facilities and operations. SPU implements an all-inclusive, integrated security strategy (see DSG section 15.2.4) that consists of several alerting devices to signal the Operations Response Center (ORC). SPU deploys three types of security systems: intrusion detection, access control, and closed-circuit television (CCTV) surveillance camera systems. Security Department representatives and ORC operators are responsible for assessing alarms and deploying the appropriate level of response. Security Department representatives can conduct a risk-based assessment of a property's design to determine the intrusion detection equipment most appropriate for the property. This could require a full, comprehensive risk assessment (see DSG section 15.3.2) or an individual consequence, vulnerability, or threat assessment (see DSG section 15.3.1).

15.2.3 Personal Safety

Both public and employee safety measures must be incorporated when planning SPU projects, such as facilities, infrastructure, and construction projects. SPU recommends physical property layouts and operational risk assessments to identify potential safety and security vulnerabilities.

Security measures such as proper lighting, landscaping, and entry protocols can be implemented in addition to, but not as a substitute for, regulatory and legal safety codes.

15.2.4 All-Inclusive Integrated Security Strategy

DSG sections 15.3 through 15.7 provide SPU project management teams with a deeper understanding of the Security Department's recommended optimal security considerations. Following these guidelines from the beginning of the planning and design process will help to ensure that security needs are adequately considered. Accounting for security features during initial facility design ensures that security features are more likely to be cost-effective, better integrated, and more operationally useful than those superimposed on existing structures through add-ons or change orders. Each utility, as well as each individual facility, has its own unique layout, culture, and operational environment. These factors combined with the level of risk and the available resources require an asset-specific approach.

The security strategies in the following sections represent the Security Department's guiding standards and techniques. Ongoing security assessments of plan deviations must be conducted by a Security Department representative during all stages of development.

15.3 SECURITY STRATEGY

This section details the primary tenants of SPU's security strategy, including threat and risk assessments and a summary of SPU's levels of protection for facilities and infrastructure.

15.3.1 Threats

An understanding of the threat environment associated with water systems is essential before developing a security strategy. Natural disasters and extreme weather conditions are two examples of known, constant threats. Other threats, such as malicious acts, are of great concern to public infrastructure and essential service providers. The attacks on the World Trade Center on September 11, 2001, and other terrorist attacks (including international and domestic terrorism) serve as constant reminders of the great importance of security for public infrastructure and utilities.

As the utilities and infrastructure under SPU's protection are a potential target for adversarial destruction and disruption, SPU recognizes that identifying potential threats and consequences to infrastructure is essential in maintaining public trust.

Potential malicious acts on public infrastructure can include:

- Vandalism, arson, or destruction of critical infrastructure
- Exposure to toxic substance
- Personal assault
- Use of improvised explosive devices (IEDs)
- Interruption of operations
- Theft of equipment
- Breach of customer data

- Threat-invoked public fear
- System hacking
- Use of chemical, biological, and radiological (CBR) contaminants

This is a list of only a few examples and is not exhaustive; many more potential threats exist. Malicious acts are intended to affect as many people as possible and promote public distrust. As the physical and operational features vary at each facility or infrastructure, SPU recommends that a Security Department representative conduct a risk assessment (see DSG section 15.3.2) to identify asset-specific potential threats.

15.3.2 Risk Assessment

The first step in integrating security into planning and designing a new construction project or major renovation is to request a risk assessment by a Security Department representative. The Security Department defines the risk to a facility or infrastructure as the probability of an undesirable event occurring and the capacity to address a potential loss. Using their expertise and experience, a Security Department representative will evaluate the designed plan for security vulnerabilities. The Security Department assesses physical security through a risk-based process that evaluates risk as a function of threats, vulnerabilities, and consequences. This security evaluation will include a neighborhood crime analysis, physical site inspections, and an examination of any documented occurrences at similar SPU properties.

The Security Department representative will identify general and site-specific potential threats. The consequences of identified threats and the likelihood of their occurrence will determine the amount of associated risk. Factors such as history, motivation, and the capabilities of a threat can help determine the recommended countermeasures. All types of threats must be considered during the threat assessment because the protective measures may differ per type of threat, regardless of the level of severity. Identified threats can be evaluated based on potential impact and probability, as described below:

- **Impact.** The urgency of a threat is based on the severity of the consequences.
- **Probability.** The likelihood of a threat is based on the probability of the occurrence.

The Security Department and project coordinators must meet during the initial stage of planning to discuss the risk assessment and agree upon the required level of security that best addresses identified risks. Although the level of impact on an asset is not typically in dispute, determining the likelihood of occurrence and the acceptable risk usually requires a more detailed evaluation. The consequences of accepted risk defined by the Security Department rest solely on the project's decision makers.

15.3.3 Levels of Protection

Design basis threats (DBTs) are vulnerabilities identified based on physical characteristics and projected standard operating procedures (SOPs). During the designing stages, the Security Department will conduct an initial and ongoing risk assessment of DBTs surrounding a facility or infrastructure. The Security Department will recommend design options based on the project's established level of protection and will continuously monitor the recommendations throughout the duration of the project.

Because the level of acceptable risk tolerance is subjective and can have a considerable effect on the cost and the degree to which the project undertakes security improvements, the Security Department has developed the following four risk-based levels of protection:

- Minimum protection
- Basic protection
- Intermediate protection
- Advanced protection

Each level of protection represents the amount of tolerated risk and the recommended security improvements. The Security Department defines security improvements as any physical or operational deviation that reduces the likelihood or probability of a threat. Levels of protection help determine each project's degree of accepted risk.

The subsections below detail the four risk-based levels of protection.

15.3.3.1 Minimum Protection

Minimum protection is appropriate when the project/asset is associated with the following findings based on threat and risk assessments:

- Low probability of a threat
- Low impact resulting from likely threats
- The project accepts a low risk from potential threats

This system is designed to impede (**not prevent**) unauthorized activity from potential threat elements (PTEs) such as criminals and vandals. Unauthorized activity could range from a simple trespass by foot to forced-entry burglary by hand. Minimum protection may physically delay PTEs.

15.3.3.2 Basic Protection

Basic protection is appropriate when the project/asset is associated with the following findings based on threat and risk assessments:

- Moderate probability of a threat
- Moderate impact resulting from likely threats
- The project accepts a moderate risk from potential threats

This system is designed to impede (**not prevent**) unauthorized external activity from PTEs such as criminals and vandals. Unauthorized activity could range from a simple trespass by foot to forced-entry burglary by hand. Basic protection may provide visual detection of and physically delay PTEs.

15.3.3.3 Intermediate Protection

Intermediate protection is appropriate when the project/asset is associated with the following findings based on threat and risk assessments:

- Moderate probability of a threat
- Moderate impact resulting from likely threats
- The project accepts a low risk from potential threats

This system is designed to impede (**not prevent**) unauthorized external activity from PTEs such as criminals, vandals, and insiders (those granted access to the property). Unauthorized activity could range from a simple trespass by foot to forced-entry burglary by hand or conspiracy to sabotage the project by insiders. Intermediate protection may provide visual/electronic detection and physical delay of PTEs, including assessment by and response from protection forces.

15.3.3.4 Advanced Protection

Advanced protection is appropriate when the project/asset is associated with the following findings based on threat and risk assessments:

- High probability of a threat
- High impact resulting from likely threats
- The project accepts a low risk from potential threats

This system is designed to impede (**not prevent**) unauthorized external activity from PTEs such as criminals, vandals, terrorists, and insiders. Unauthorized activity could include a simple trespass by foot, forced-entry burglary by hand, conspiracy to sabotage by insiders, or terrorism. Advanced protection may provide visual/electronic detection and physical delay of PTEs, including assessment by and response from protection forces.

15.4 SECURITY SYSTEM DESIGN

Designing a security system requires identifying threats to critical assets and associated risks. Owners and operators must employ a comprehensive physical protection system (PPS) to mitigate these risks. SPU urges architects, planners, and designers for projects to evaluate and consider all potential security solutions for a project before selecting the approach that best addresses their needs in a responsive and cost-effective manner. The Security Department will provide a rationale for each approach it recommends, with the expectation that project managers and owners provide a rationale for each recommendation not selected. Proper PPSs combine people, procedures, and equipment into a single methodology. SPU implements an all-inclusive, integrated security system using a unified security software program known as American Magnetics (AMAG) (see DSG section 15.6.2.1). An AMAG system is developed by evaluating how a facility or infrastructure may be targeted and establishing proper countermeasures to prepare, deter, detect, delay, and respond, as described in further detail below:

- **Prepare.** Assuring that all security measures are functioning properly, including personnel such as monitoring centers and emergency responders.

- **Deter.** Visible security features, such as fencing, surveillance cameras, intrusion detection sensors, and protective lighting, may deter an adversary from acting against an asset. These observable layers of protection can prevent minor incidents like vandalism and theft before they occur.
- **Detect.** Security measures, such as intrusion detection systems, monitored video surveillance systems, access control systems, and protective lighting, may assist in detecting and assessing a security incident. Detection equipment is only as strong as the people evaluating and responding.
- **Delay.** Implementing physical security measures, such as locks, fencing, and other Crime Prevention Through Environmental Design (CPTED) obstacles, can impede an adversary's rate of advance. These delay measures can disrupt a PTE's progress in attacking or disrupting an asset until security responders arrive to neutralize the incident.
- **Respond.** Incident response time depends on accurate communications between those assessing the detected incident and the response force. Understanding who must respond to the incident and how long it will take them to get there can influence the implementation of security measures. Stronger delay measures may be required for remote areas with longer expected response times.

15.5 PHYSICAL SECURITY MEASURES

This section details the different types of physical security measures available for protecting SPU projects and property, as well as SPU security recommendations for implementing each security type. Security recommendations do not substitute, but must act in addition to, any regulatory and legal safety codes.

15.5.1 Crime Prevention Through Environmental Design

CPTED strategies rely on altering the physical and environmental design to deter criminal behavior by influencing PTE's decisions before they commit a criminal act. Implementing CPTED barriers is cost effective and reduces criminal opportunity. Though CPTED measures vary at each property based on the property's design and operating conditions, SPU has applied the following common examples at its properties:

- **Natural surveillance** deters crime by incorporating physical features in the project design to improve the general visibility at a site, increasing the likelihood that the surrounding public would observe, and thus deter, PTEs. Examples of natural surveillance include the following:
  - Streets and sidewalks to increase pedestrian traffic
  - Large windows with open shades
  - Points of entry in high-traffic areas
  - Additional lighting
  - Landscaping designed to provide surveillance
  - Pedestrian entrances adjacent to vehicle entrances

- **Natural access control** limits unwanted traffic by incorporating physical features in the project design that discourage access to restricted areas. Examples of natural access control include the following:
  - Limited points of entry
  - Thorny plants or bushes near fences or windows
  - Diversion landscaping
  - Restricted access to roofs from adjacent buildings, dumpsters, fences, and poles
- **Natural territorial reinforcement** deters crime by incorporating physical features in the project design that dissuade PTEs through public presence and social control. Examples of natural territorial reinforcement include the following:
  - Physical features that encourage community activities
  - Amenities such as seating and restrooms
  - Parks on-site

15.5.2 Fencing

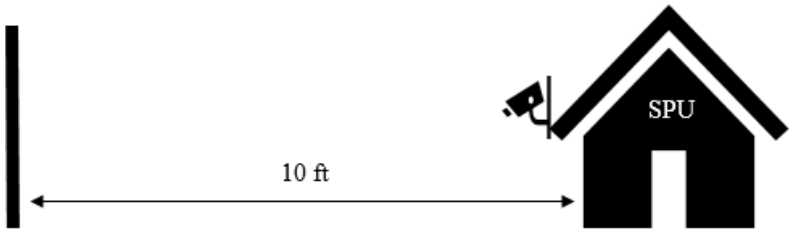
Fencing is often referred to as the first line of defense and is one of many equipment elements contributing to a PPS. Fencing establishes a perimeter boundary and barrier to a facility, requiring potential intruders to make an overt action to penetrate and thereby demonstrating intent. Fencing can deter, prevent, and delay unauthorized access. In addition, fencing can shield a facility from visual observation and create a standoff clear zone, an area providing an unobstructed line of sight where an intrusion detection sensor can be installed. Fencing designed to simply give notice of legal boundary is not considered a security measure. The Security Department will recommend specific fencing types based on the defined level of protection for a project. The specific security standards for fencing and types of fencing are detailed in the subsections below.

When choosing a fence, the public's expectation of style and consistency should be considered. Park-like or residential neighborhood settings call for placing importance on aesthetic style when determining appropriate fencing.

15.5.2.1 Standoff Distance between Fence Line and Infrastructure

The Security Department recommends a minimum standard of a 10 feet (ft) standoff distance between all sides of an infrastructure and the fence line (Figure 15-1). Standoff distance refers to measures to prevent unscreened and potentially threatening people and vehicles from approaching within a certain distance of the infrastructure. This standard applies to all levels of security, though higher levels of protection may require a greater distance between the fence line and the infrastructure. The distance, and thus time, combined with a high level of visibility offered by standoff distance reduces the likelihood of an intruder. In addition, the standoff distance can reduce the resulting damage from a vehicle's impact at high speed.

Figure 15-1
Standoff Distance



15.5.2.2 Fencing Foundation and Enhancements

The Security Department standards require that all fencing fabric must extend to within 2 inches of firm ground. The fabric must be anchored to prevent PTEs from lifting the fencing by hand more than 5 inches. In selected areas, DBTs may necessitate a continuous concrete curb at the base of the fence. This fencing enhancement may prevent a PTE from digging under the fence line. Tunneling prevention such as a concrete curb must be used in areas containing soft soils.

If there is an area where the fence line crosses drainage culverts, utility underpasses, streams or other openings, the area must be secured by adding additional fencing, grills, or other barriers to discourage penetration without impeding the utility or infrastructure.

15.5.2.3 Fencing Toppers

All fencing options recommended by the Security Department also include fencing topper requirements. Toppers supplement fencing intrusion protection by posing as an additional layer of defense to deter and delay infiltrations. Examples of SPU Security recommended toppers are shown in Figures 15-2 through 15-4 below.

Figure 15-2
Barbed Wire

Figure 15-3
Concertina Razor Wire

Figure 15-4
Estate Style Defenders

15.5.2.4 Chain-Link Fencing

Chain-link fencing establishes a perimeter barrier and can deter and delay intrusion. Security Department's basic level of protection (see DSG section 15.3.3.2) recommends 7-ft galvanized steel fencing along with a 1-ft barbed or razor wire topper (see DSG section 15.5.2.3). Pros and cons to chain-link fencing are as follows:

- **Pros:**
  - Low maintenance
  - Concealment
- **Cons:**
  - Scalable
  - Easily cut

Figure 15-5 below is an example of chain-link fencing protecting an SPU asset.

Figure 15-5
Chain-Link Fencing

15.5.2.5 Estate Ornamental Fencing

Estate fencing establishes an aesthetically pleasing perimeter barrier. It is a better deterrent than chain-link fencing, as it provides greater resistance to climbing. Security Department's intermediate and advanced levels of protection recommend estate fencing with 7-ft iron rod, 18-gauge pickets spaced at 5 inches. A 1-ft straight or curved topper is also recommended (see DSG section 15.5.2.3). Pros and cons to estate ornamental fencing are as follows:

- **Pros:**
  - Climb resistant
  - Prestigious look
- **Cons:**
  - Rigid structure

Figure 15-6 below is an example of estate ornamental fencing protecting an SPU asset.

Figure 15-6
Estate Ornamental Fencing

15.5.2.6 Anti-Cut and Anti-Climb Fencing

Critical assets with a warranted DBT should consider anti-cut and anti-climb fencing, which provides a higher level of intrusion deterrence. The Security Department's advanced level of protection recommends 9-wire gauge mesh with 5/8-inch mesh pattern. A 1-ft barbed or razor wire topper is also recommended (see DSG section 15.5.2.3). Pros and cons to anti-cut and anti-climb fencing are as follows:

- **Pros:**
  - Climb resistant
  - Cut resistant
- **Cons:**
  - Defending presence

Figure 15-7 below is an example of anti-cut and anti-climb fencing protecting an SPU asset.

Figure 15-7
Anti-Cut and Anti-Climb Fencing

15.5.3 Security Gates

Security gates are barriers that limit or restrict public access to or from an asset in accordance with identified facility requirements. Security gates are designed to direct pedestrian and/or vehicle circulation to and from an area. Gate installation must meet the same or greater security standards as adjacent fencing. When determining the gate type most suitable for an asset, project managers should consider factors such as pedestrian and vehicle traffic flow, types of vehicles, and the facility's operation plans. Physical gate components include the frame, top guard, fabric, hinges, latches, operators, and locking devices. Security Department recommendations regarding these components are as follows.

- The frame, fabric, and top guard should match the surrounding fencing aesthetically and in the level of protection provided (see DSG section 15.5.2) when applicable. Stand-alone gates used will depend on the protected asset or restricted road.
- Per Security Department standards, swinging and sliding gates are the only two gate types recommended at this time. Both can be made as either a single or double gate, depending on accessibility needs.
- Latches and locks depend on the facility's design and needs and whether the gate will be integrated into the security control system.

15.5.3.1 Ranch Gate

In specific circumstances to control vehicle access, the Security Department recommends ranch gates. Though not built to protect against pedestrian traffic, ranch gates are constructed using steel to deter vehicle access on restricted roads. Figure 15-8 below is an example of a ranch gate used on SPU property.

Figure 15-8
Ranch Gate

15.5.3.2 Automated Gate Operators

As stated in DSG section 15.5.3.2, swinging and sliding gates are the only two methods of operation recommended at this time. Automated gate operators can open and close both swinging and sliding security gates. These operators can be integrated into a security system and

controlled remotely, offering an efficient method of restricting access to a gated area. The Security Department currently recommends two automated gate operators (HySecurity Swingsmart DC 20 ,HySecurity Slidesmart DC 15, and HySecurity SlideSmart HD see Figures 15-9 and 15-10 below) based on the following standards and requirements:

- The Security Department recommends adherence to the UL 325 standards, a safety standard designated by the American National Standards Institute (ANSI), which state that all gate operators are required to have a minimum of two independent means of entrapment protection where the risk of entrapment or obstruction exists. To meet this requirement, a gate opener can use two inherent-type systems, two external-type systems, or an inherent and an external system. Although these specific safety measures are determined after evaluation of the fence and gates, they may include loop detectors, edge detectors, and photo eyes.
- Facility designs should prevent and discourage pedestrian use of vehicle exit gates as the primary means to exit a property.

Figure 15-9
HySecurity Swingsmart DC 20

Figure 15-10
HySecurity Slidesmart DC 15

Figure 15-11
HySecurity Slidesmart HD

15.5.4 Anti-Ram Vehicle Barriers

Depending on the DBT, vulnerable areas in the perimeter surrounding an asset may require additional barriers to prevent high-impact vehicle penetration. The Security Department recommends anti-ram protected gates and bollards on all exposed vulnerable areas based on

the identified DBTs. These methods should act in addition to any CPTED and standoff distance, not alone (see DSG section 15.5.2.1). Fencing alone is not considered sufficient protection against a moving vehicle attack. Most fencing can be easily penetrated by a moving vehicle and will resist impact only if reinforcement is added.

15.5.4.1 Anti-Ram Protected Gates

Anti-ram protected gates are restrictive barriers designed to resist vehicle penetration. The protection methods depend on the type of gate installed but typically consist of impact-resistant poles that reinforce the gate, allowing it to absorb kinetic energy.

Figure 15-11 below is an example of anti-ram protected gates.

Figure 15-11
Anti-Ram Protected Gate

15.5.4.2 Bollards

Bollards are anti-ram posts cemented into the ground to provide protection against vehicle impact. They should be positioned in vulnerable areas and individually engineered for soil conditions. The Security Department implements these cement barriers to prevent vehicles from approaching the barrier at high speeds.

15.5.5 Security Lighting

Security lighting, especially in parking lots, improves visibility when natural light is limited, increasing capabilities to detect, delay, and respond to unwanted activities. Lighting should be installed in a manner that enables employees to observe individuals at night from distances of 75 ft or more and to identify a human face at a distance of 33 ft. Security lighting also increases the effectiveness of guard forces and CCTV by enhancing visual range. The design of each project presents its own security challenges based on physical layout, terrain, atmospheric conditions, and security requirements. The Security Department recommends that all points in parking lots be illuminated using at least two, preferably four, lighting pole locations. The

Security Department recommends adhering to the following guidelines when installing security lighting at a facility:

- Lighting should be mounted at a minimum height of 20 ft and provide a minimum of 5 foot-candles (the degree of illuminance provided by the security lighting) surrounding key assets.
- Lighting at entry and exit points should provide at least 10 foot-candles for safety.
- Lighting in general roadways and parking areas should illuminate 5 to 10 foot-candles.
- Areas planned to include CCTV camera coverage should include lighting that illuminates 5 to 10 foot-candles.
- General outdoor areas should be illuminated to 5 horizontal foot-candles.
- Motion-activated lighting should be installed where applicable.
- All lighting must be directed away from the infrastructure to avoid interfering with property surveillance.
- Additional lighting depends on a Security Department assessment of both DBTs and countermeasures.

Consult with local code officials for additional restrictions that may apply to the security lighting levels.

15.5.6 Security Signage

Installing security signage, even in some non-required locations, deters PTEs by clearly indicating the boundary and presenting the consequences for violation. The Security Department recommends placing standard security signage at facility entrances and along fence lines for facility identification and public safety. Signage should be designed to draw attention and be stylistically consistent with other SPU signage whenever possible. Below are examples of SPU's recommended security signage. Figure 15-12 provides examples of SPU security signage.

Note: *Signage should be designed in accordance with Seattle's Sign Code (Seattle Municipal Code [SMC] 23.55).*

Figure 15-12
Security Signage Examples

SPU Before Leaving Sign

SPU Gate Remain Closed Sign

SPU For Access Sign

SPU Secured Facility Sign

SPU SCADA Sign

SPU Before Leaving/Entering Signs

SPU Main Entry Sign

SPU No Trespassing Sign

SPU Remain Closed Sign

15.6 ELECTRONIC PHYSICAL SECURITY EQUIPMENT

Physical security equipment can assist in intrusion detection, access control, and property surveillance. The type of security equipment recommended by the Security Department depends on many factors, including the agreed upon level of protection, resolution goals, type of asset, and the history, motivation, and vulnerabilities at the facility.

Security standards and recommendations do not substitute, but must act in addition to, regulatory and legal safety codes.

15.6.1 Critical Utility Connections

The availability of essential elements such as a power supply, wiring, and networking will govern the security system's overall capabilities. All utilities need to be protected from inadvertent or deliberate damage that could interfere with operations. Preliminary discussions must take place early in a project's life cycle to avoid future conflict among different disciplines. Coordination among project representatives contributes to the success of building an effective security

system. The Security Department's Capital Projects Coordinator will assist in ensuring that security design elements are incorporated into the initial planning phases.

15.6.1.1 Power Supply

A reliable power source is essential in the development of a successful security system. Strategies for powering the security structure in addition to preventing power interruption must be implemented early in a project's life cycle. SPU security devices require numerous junction boxes and conduit pathways. Coordination between the Security Department, electrical contractor, and security vendor will ensure the project's efficiency. The Security Department's baseline power supply recommendations are as follows:

- All core power lines entering a facility must be hardened to prevent interruption.
- Electrical wiring must be protected within a project's pre-determined level of conduit. All exposed conduit must be galvanized rigid. The underground conduit can be polyvinyl chloride (PVC) Schedule 80.
- All boxes must be heavy cast; pot metal boxes are not permitted.
- Substitutions must be submitted to and approved by the Security Department.
- Neither conduit nor junction boxes should be labeled with security signage as doing so may encourage tampering.
- A backup power source must be implemented in all physical security plans (generators, uninterruptible power supplies [UPSs], Solar battery back-up, or battery units).
- Unoccupied facilities should not have exposed wiring.

15.6.1.2 Wiring

When new or major renovation projects are being designed, the project team must determine pathways for wiring to and from security devices with architects and structural engineers. Planning must include implementing strategies to prevent any power or communication interruptions early on in a project's development. The Security Department's baseline wiring recommendations are as follows:

- All security wiring must be protected within the project's pre-determined level of conduit. All exposed conduit must be galvanized rigid. The underground conduit can be PVC Schedule 80.
- All exterior security device conduit must be concealed where possible. Interior exposed wiring depends on the facility or infrastructure.
- Pathways to security devices must be provided.
- Neither conduit nor boxes should be labeled with security signage as doing so may encourage tampering.
- Conduit must offer additional spare space for future changes and additions.
- Unoccupied facilities should not have exposed wiring.

15.6.1.3 Networking

A communication method for transmitting the security systems data must be established early on in a project's development. Network communication is essential to providing 24/7 remote surveillance and monitoring for critical assets. This includes retrieving all the data from gate

operators, motion detectors, and door sensors. The Security Department recommends fiber optic networking cables as they provide the much-needed data capacity and have fewer failures than other restricted communication methods. Early coordination with the City of Seattle's Information Technology (IT) Department or any predetermined service provider is essential.

15.6.2 Access Control System

An access control system grants access to authorized personnel while detecting or delaying access to unauthorized persons. In addition to CPTED measures (see DSG section 15.5.1), electronic devices such as card readers, door controllers, request-to-exit devices, electric strikes, motion detectors, magnetic contacts, and intercom systems can be strategically installed to regulate admittance and access to an area. Typically found at entry points to a facility itself, access control systems are also used to protect restricted areas within a facility as well. These devices allow automated verification to grant or deny a person access to an area. Refer to **Appendix 15A - Construction/Maintenance Projects Site Security Plan** for guidance on setting access control rules for contractors and vendors.

15.6.2.1 American Magnetics Security System

The Security Department uses an AMAG security system as part of its all-inclusive integrated security management system (see DSG section 15.4). AMAG is a unified security software program that allows the Security Department to access and control all deployed devices using a single interface. This system incorporates control of intrusion detection, access, video, identity verification, and visitor management throughout SPU-managed properties and facilities. SPU-authorized personnel can remotely access a web client computer containing the AMAG security software to perform system-wide managing tasks. The system continuously monitors all SPU Security device activities, such as alarms or security events, and records data from the event into the system's database unit (DBU).

15.6.2.2 Controllers

Controllers, also called nodes, store and manage the data necessary for operating the AMAG security system. Nodes store all imported access control relevant rules and manage all the connecting devices. The Security Department recommends several different types of controllers, depending on infrastructure layout and device needs. Because controllers typically consist of multiple modules and other expansion options, the Security Department recommends that the project team determine the location and installation of the controller early in the project design process. When planning the installation of a security management system controller, the Security Department recommends the following best practices:

- Ensure available space to accommodate all controller cabinets.
- Confirm that proper cabling routes are available, paying special attention to maximum lengths.
- Ensure that essential utilities, such as networking and power, are available.
- Install a tamper switch on all security panel enclosures.

15.6.2.3 Card Readers

Card readers enable authorized personnel to verify access privileges. The card reader scans card numbers and forwards the information to the controller. The controller then determines

whether access is to be granted based on stored data for the specified card number. If access is granted, the controller sends a signal releasing the locking mechanism (electric strike, magnetic lock, or gate operator). The Security Department recommends the following best practices for installing card readers:

- Install card readers on doors and gates leading to critical assets or restricted areas.
- Install card readers adjacent to the controlled door or gate.
- Card readers should be HID Global's (HID's) Signo with a red-light emitting diode (LED) that turns green upon entry, unless otherwise specified by the Security Department.

15.6.2.4 Exit Devices

Depending on operational needs and security expectations, the Security Department recommends multiple types of exit devices, including passive infrared request to exit, push pads, or exit loops. These devices are used to detect individuals exiting a facility or area. Exit devices sometimes activate a relay switch to unlock the door and disarm an alarm system when a person is exiting.

15.6.2.5 Electric Strikes

Electric door strikes enable the electrical release of a door's lock, latch, or bolt. The Security Department recommends specific electric strike devices based on the project's door plans.

15.6.2.6 Keypad Locks

The type of keypad lock will depend on the operational needs and security expectations of a facility. The most common type of keypad lock used by SPU is a numeric keypad lock, which is a programmable keypad requiring the user to enter a code before the door or gate will unlock.

15.6.2.7 Contacts

A contact is an alerting device generally mounted on doors, gates, hatches, cabinets, or vents to monitor points of entry. The device can detect when and how long the monitored point is open. This data can help determine whether the point of entry is being forced or held open. The types of contacts recommended for a project will depend on the operational needs and security expectations of the facility. Doors and windows that offer access to restricted areas can be monitored and set with an alarm to alert security personnel of any unauthorized entry.

15.6.2.8 Motion Detectors

Motion detectors are devices mounted within a certain area to detect movement. The types of motion detectors recommended for a project will depend on the operational needs and security expectations of the project. The area of coverage can be tailored to best protect the asset.

15.6.2.9 Intercoms

An intercom is a device typically installed in a controlled point of entry. Intercoms allow security operators to speak to individuals requesting access to an area. After verifying the requester's identification, operators can locally or remotely grant or deny access.

15.6.3 Video Surveillance

The Security Department implements a comprehensive CCTV system consisting of hundreds of strategically placed cameras. Cameras deter and detect unauthorized entry and provide forensic video evidence for investigations following a crime against SPU property. The Security Department employs an assortment of cameras, digital video recorders (DVRs), video switches, and viewing monitors, providing both local and remote access. These cameras are integrated into the AMAG system, allowing operators to monitor activity from SPU's security control center. Performance specifications differ with each device but can include scheduled, alarmed, or manual-triggered actions as well as video analytical programming. SPU currently deploys cameras that are either fixed (Figure 15-13) or capable of remote, directional, and zoom control, such as pan-tilt-zoom (PTZ) or dome cameras (Figure 15-14). Each camera offers a different field of view and is determined based on DBTs as they relate to mutually established resolution goals.

Figure 15-13
Fixed Camera

Figure 15-14
PTZ/Dome Camera

The Security Department recommends surveillance devices based on DBTs as they relate to mutually established resolution goals, suitability based on operational needs, site conditions, and availability of local area networks. The Security Department will provide ongoing assessments as to which cameras will best fit each operating environment based on necessary positioning, field of view, light compensation, housing, and mounts. Early communication with the Security Department is important in determining the power, networking, and wiring requirements for video surveillance installation at a facility.

15.7 COST IMPLICATIONS

Early coordination among project managers and the Security Department is imperative in designing an all-inclusive, cost-effective PPS. Though total costs depend on an assortment of varying factors, physical security measures should correspond with the project's agreed level of protection (see DSG section 15.3.3). Other factors that must be considered and may affect total cost include equitable residential aesthetics, future expansion abilities, and maintenance conditions.

15.8 RESOURCES

Removed for Security