This document is released for the purpose of information exchange review and planning only under the authority of Tracy Anne Clinton, September 2017, State of California, PE No. 48199

City of Oxnard

Public Works Integrated Master Plan

OVERALL

PROJECT MEMORANDUM 1.5
SECURITY OF UTILITIES FACILITIES

REVISED FINAL DRAFT
September 2017

Engineers...Working Wonders With Water®

2700 YGNACIO VALLEY ROAD • SUITE 300 • WALNUT CREEK, CALIFORNIA 94598 • (925) 932-1710 • FAX (925) 930-0208

PREFACE

The analysis and evaluations contained in these Project Memorandum (PM) are based on data and information available at the time of the original date of publication, December 2015. After development of the December 2015 Final Draft PMs, the City continued to move forward on two concurrent aspects: 1) advancing the facilities planning for the water, wastewater, recycled water, and stormwater facilities; and 2) developing Updated Cost of Service (COS) Studies (Carollo, 2017) for the wastewater/collection system and the water/distribution system. The updated 2017 COS studies contain the most recent near-term Capital Improvement Projects (CIP). **The complete updated CIP based on the near-term and long-term projects is contained in the Brief History and Overview of the City of Oxnard Public Works Department's Integrated Planning Efforts: May 2014 – August 2017 section.**

At the time of this Revised PWIMP, minor edits were also incorporated into the PMs. Minor edits included items such as table title changes and updating reports that were completed after the December 2015 original publication date.

City of Oxnard

Public Works Integrated Master Plan

OVERALL

PROJECT MEMORANDUM 1.5
SECURITY OF UTILITIES FACILITIES

TABLE OF CONTENTS

Page No.

SECURITY OF UTILITIES FACILITIES

1.0 INTRODUCTION

As part of the Public Works Integrated Master Plan (PWIMP), Summers Associates, LLC was contracted to develop a basis of design for physical and electronic security for all the City of Oxnard (City) facilities and to identify existing deficiencies in existing facility security. The draft reports can be found in Appendix A and B.

1.1 Project Memorandums (PMs) Used for Reference

Other Project Memoranda (PMs) that relate to the security effort include:

- PM 1.1 - Overall - Master Planning Process Overview.
- PM 2.1 - Water System - Background Summary.
- PM 3.1 - Wastewater System - Background Summary.
- PM 4.1 - Recycled Water System - Background Summary.
- PM 5.1 - Stormwater System - Background Summary.

2.0 FINDINGS

Appendix A provides general recommendations and details for utility security measures.

Appendix B provides a set of guidelines for enhancing security of City facilities during their design and construction. Threats considered include common crime, terrorist attacks, other manmade hazards, as well as some natural hazards. Cost effective recommendations are outlined in each section to enhance safety throughout a facility's lifetime. These recommendations apply to both new facilities as well as additions and modifications to existing facilities.

Appendix C provides a physical security needs assessment, including strengths and weaknesses with recommendations for improving conditions, of the City's Maintenance Service Center.

This PWIMP assumes that the costs of the proposed security measures are included in the planning contingency for each CIP project. Security measures are not included in the CIP as a separate line item.

APPENDIX A – UTILITIES OVERALL SECURITY SUMMARY FINDINGS AND RECOMMENDATIONS

CITY OF OXNARD CALIFORNIA

Public Works Integrated Master Plan

Utilities Overall Security Summary Findings and Recommendation

FINAL DRAFT

December 2015

Prepared for:

carollo
Engineers...Working Wonders With Water™

Prepared by:

Summers Associates, LLC
"Making our world a safer place by design"

CITY OF OXNARD

Public Works Integrated Master Plan

Utilities Overall Security Summary Findings and Recommendations

TABLE OF CONTENTS

Page No.

1.0 INTRODUCTION

The following observations were made by the assessment team based upon a review of architectural plans, meetings with key personnel, and personal observations at the assessment locations. The observations are not listed in order of priority. The findings and recommendations are limited to the evaluation of the current state of physical security systems and its ability to detect intrusion by a human adversary. If inadequate, recommendations are made to enhance the respective physical security system. As a precautionary measure against unauthorized distribution, the level of detail describing noted deficiencies, conditions or locations has purposefully been generalized or omitted due to the sensitive nature of this information. Employees familiar with these locations will garner sufficient information necessary to understand and implement the included recommendations. For these reasons, photographs have not been included to further illustrate the deficiency.

1.2 FINDINGS AND RECOMMENDATIONS

1.2.1 Water Campus

Findings

A. The perimeter approximate 2,800' perimeter of the Water Campus is a hodgepodge of fencing and wall materials that does not comply with base-level fencing guidelines cited by ANSI/ASCE/EWRI 56-10. Materials currently in use include black ornamental aluminum fencing, cinder block walls, and chain-link fencing that is only 5-feet-tall in some of the most vulnerable locations along the perimeter. Some of the perimeter fencing has topping materials such as barbed or concertina wire, but most does not. There is widespread evidence of jumping and some cutting of the chain-link fence fabric.

B. A review of security operations center activity logs for a 26-month period of April 2013 to June 2015 shows 90 incidents of trespassers—frequently noted as "jumpers" in the security activity log. When there is a colloquial expression used by security personnel to describe a specific activity, there is clearly a problem that is not being addressed. In short, the perimeter of this critical infrastructure facility can be best described as *porous*. To compensate for this lack of a sufficient perimeter, the campus must rely on video surveillance and private security when a properly constructed perimeter fence or wall would prevent the overwhelming number of trespassing events. Chain-link fence fabric is far too easy to scale and cut. Due to regular trespassing incidents onto the campus, considerable criminal activity within close proximity, and the nature of adjoining properties (1,100' fence line with railroad property), replacement of chain-link with a welded steel fence panel system is recommended.

RECOMMENDATION: Immediate consideration should be given to establishing a firm perimeter utilizing an 8' high welded metal fence panel system such as the Ameristar Montage II (installed at the AWFP). For existing cinder block walls, 3' high versions of welded metal fencing panes such as the Montage II should be mounted on top of the walls to significantly minimize or eliminate scaling. For guidance on the selection of anti-climb, anti-cut fencing, see ANSI/ASCE/EWRI 56-10, Appendix 1.2.

C. While the facility is equipped with numerous cameras, both exterior and interior, video surveillance coverage is inadequate in several areas within the perimeter, particularly west of the 3rd Street Bridge. Day/night fixed position and pan, tilt, zoom (PTZ) camera coverage should be added to provide comprehensive perimeter coverage and subsequently enhance real time detection and response by the security operations staff.
Several cameras were noted to be non-functional. In general, the majority of cameras are functional but nearing end of life cycle phase. Older model cameras do not perform well in low light conditions.
RECOMMENDATION: A comprehensive camera replacement phasing plan should be prepared and implemented as soon as feasibly possible.

D. The Water Campus is home to the Water Section Security Office. The office is staffed by an around-the-clock private security officer. A video surveillance monitoring station is located inside the Water Section Security Office. From this computer terminal, security officers are able to monitor video feeds from not only the water campus but several blending stations and a lift station. This area is also utilized to process individuals visiting the Water Department.
RECOMMENDATION: This area should be redesigned to allow for monitoring of all Utilities future video surveillance systems and alarm verification. It should eliminate uncontrolled access to the monitoring area but allow for public interaction and eliminate opportunities to view the monitoring area from outside the facility, particularly at night.

E. An outdate proximity card reader system is utilized for perimeter door control. The majority of doors are either missing door contacts or the door contacts are not connected to the access control system. This eliminates opportunities to monitor the building perimeter doors and to detect a "door held open" or "door forced open condition." This condition results in complete reliance of the video surveillance system as the sole source to detect unauthorized entry. Video surveillance systems should respond to and supplement perimeter/interior alarm systems/activations and not be used in place of them from a concentric layer of protection standpoint. Additionally, ground level office windows are vulnerable to forced entry. No motion detection or acoustic/seismic detection devices exist to detect forcible entry.
RECOMMENDATION: The access control system should be replaced with a comprehensive design utilizing Software House Access Control with integrated intrusion detection and Milestone to ensure system compatibility with Oxnard PD.

F. Numerous perimeter door lock latching mechanisms were found to be vulnerable to tampering and forced entry.
RECOMMENDATION:
All perimeter doors should be equipped with protective metal latch-guards to restrict access. Ensure door hinges are properly pinned to prevent removal. Whenever possible, utilize internal door hinges, such as piano hinges, to minimize hinge tampering.

G. Minimum signage was noted along the perimeter resulting in limited territorial reinforcement.
RECOMMENDATION:
Post signage prohibiting trespassing every 50' along perimeter fencing, especially that which abuts railroad property. See ANSI/ASCE/EWRI 56-10 Appendix 1.2 for signage recommendations.

H. Perimeter Lighting – The Water campus lighting system suffers from inconsistent uniformity ratios. While some areas are adequately illuminated, other areas are barely illuminated.
RECOMMENDATION: A comprehensive campus photometric study be conducted to establish an action plan to bring campus lighting in compliance with ANSI/ASCE/EWRI 56-10.

1.2.2 Advanced Water Purification Facility

Findings

A. The facility perimeter is designated by an 8' tubular metal fence with no horizontal foot-hold opportunities by vendor Ameristar which provides good anti-climb protection with excellent natural surveillance opportunities. Unfortunately, this fence type was only used at the front of the facility at the northwest gate and along the west side of the perimeter. The remainder of the facility is equipped with 6' chain link fence topped with 3 horizontal rows of barbed wire. Due to the grade of the terrain in certain areas of the perimeter, the fence height is reduced to approximately five feet.
RECOMMENDATION: Replace vulnerable chain link fence with matching 8' tubular metal fence already in existence at AWPF.

B. The large vertical chemical storage tanks located outside and adjacent to the facility's primary vehicle entry gate are partially enclosed via a metal mesh panel system. This system minimizes opportunities for an explosive device(s) to be thrown in between the tanks. It also would serve as a second line of defense from a concentric layer of protection standpoint if it were to be expanded to complete enclosed all tanks and be secured.
RECOMMENDATION:

Consider expansion of the metal mesh system to completely enclosed the said tank area and include pedestrian access doors equipped with door position switches and card readers to be integrated into the proposed security management system.

C. A manually controlled vehicle gate has been installed on the south side of the building. The gate is located between the exterior pedestrian pathways and the fire exit stairwell leading downstairs from the second floor conference room. Individuals exiting down the stairwell would find themselves on the "secured" or restricted side of the perimeter versus the publicly accessible side of the campus.
   RECOMMENDATION:
   Relocate the gate toward the restricted side of the campus so that the fire stairwell egress deploys on the unrestricted side of the vehicle gate.

D. The facility is equipped with exterior and interior ladders which are not equipped with lockable ladder guards to prohibit unauthorized access. This condition simplifies unauthorized access to equipment levels on the interior and roof access on the exterior, presenting a security and general liability exposure.
   RECOMMENDATION: Install lockable ladder guards to mitigate unauthorized access and liability exposures.

E. The facility is not equipped with any form of electronic security or video surveillance systems. A facility wide design including a Software House integrated access control system with partitioned intrusion detection and interior/exterior Pelco video surveillance cameras was recently submitted for consideration to the Oxnard Public Works Department. Vendors mentioned were selected to match existing city legacy systems including those at city facilities and Oxnard PD.

F. Critical infrastructure rooms such as IT, Labs and the Control Room should be located within the interior portions of any facility in compliance with the application and benefits associated with multiple layers (levels) of protection. At the AWPF, these rooms are located on the ground level building perimeter with floor to ceiling glass windows making them highly vulnerable to undetected vandalism, tampering or destruction.
   RECOMMENDATION:
   Apply Mylar burglary-resistant film secured in the frame (preferably) to minimize and delay forcible entry exposures. Consider darkest possible window tint to minimize the ability to observe room assets from the outside looking in. The proposed intrusion detection system design calls for the installation of dual acoustic / seismic detectors in all first floor rooms equipped with glass windows as a second layer of protection.

G. Tree growth along the Perkins Road portion of the building is negatively impacting exterior lighting uniformity ratios along with natural surveillance lines of sight. Furthermore, on

several occasions window panes have been shot out. Proposed video surveillance cameras will provide limited to zero deterrence or forensic value under existing conditions.

RECOMMENDATION: Consider removal of trees and replace with drought tolerant ground cover plants to increase illumination levels and eliminate conflict with line of sight and future surveillance cameras proposed field of views.

1.2.3 Wastewater Treatment Plant

Findings

A. The facility's primary electrical switch gear, located along the Perkins Road facility perimeter, is vulnerable to intentional/unintentional vehicle incursion. No bollards, structural or natural access control barriers exist to mitigate vehicle breach. Should this critical infrastructure be destroyed and with no redundant power source, the facility will be unable to sustain operations even with the use of its emergency generators.
RECOMMENDATION: Multiple layers of vehicle incursion solutions should be considered to mitigate this threat to critical infrastructure. Bollards, jersey barriers, decorative planters, or other vehicle barriers, where applied, should be capable of stopping a 4,000-lb (1,800-kg) vehicle traveling at 30 mph (48 km/h) within 3 ft. (0.9 m) or less as a minimum. Redundant power and emergency backup power should also be reevaluated in accordance with ANSI/ASCE/EWRI 57-10. Video surveillance coverage of this area should be included and the chain link fence, which is partially missing portions of its barbed wire topping, should be upgraded to tubular metal fencing as previously recommended in this report. Future facility designs should consider locating critical infrastructure within the center of the campus grounds to provide for multiple layers of protection and increased opportunities to detect, deter, delay and responded to threats by adversaries.

B. The facility perimeter is established by a 6' chain link fence with 3 horizontal strands of concertina wire on top. Approximately 75% of the perimeter fence is covered by dense green plant and tree growth providing no clear zones and significantly impacting natural surveillance line of site. Several incidents of individuals hoping the fence as a short cut have been reported.
RECOMMENDATION: Maintain a clear zone on both sides of the fence by removing ground cover growth on and near the fence. Remove trees and or branches that may be used as a climbing aid and maintain all branch height at 12' or higher.

C. Two of five perimeter gates are monitored by video surveillance cameras. A third gate camera is no longer functional. No other video surveillance exists on the facility grounds.

RECOMMENDATION: Provide a video surveillance system in compliance with the PWIMP Security Concept of Design. At a minimum, provide coverage of all vehicle entry points and critical core assets.

D. Buildings are not equipped with any form of intrusion detection or electronic access control.
RECOMMENDATION: Install an access control system with integrated intrusion detection in compliance with the PWIMP Security Concept of Design for the Administration Building and other critical core assets where feasible.

1.2.4 Wastewater Treatment Headworks Facility

Findings

A. Buildings are not equipped with any form of intrusion detection or electronic access control.
RECOMMENDATION: Install an access control system with integrated intrusion detection in compliance with the PWIMP Security Concept of Design.

B. No video surveillance exists on the facility grounds.
RECOMMENDATION: Provide a video surveillance system in compliance with the PWIMP Security Concept of Design. At a minimum, provide exterior coverage of all four sides of perimeter.

C. Two 480V electrical transformers are vulnerable to unintentional vehicle breach.
RECOMMENDATION: Install concrete filled metal bollards to protect this critical asset from unintentional vehicle breach in compliance with ANSI/ASCE/EWRI 57-10.

D. Critical asset rooms located on the facility perimeter are equipped with glass windows and exposed door lock latches.
RECOMMENDATION: All perimeter doors should be equipped with protective metal latch-guards to restrict access. Ensure door hinges are properly pinned to prohibit removal from the exterior. Whenever possible, utilize internal door hinges, such as piano hinges, to minimize hinge tampering. Apply Mylar burglary-resistant film secured in the frame (preferably) to minimize and delay forcible entry exposures. Consider darkest possible tint to minimize ability observe rooms assets from the outside looking in. Alternatively, consider a solid metal door replacement.

E. The facility perimeter is established by a 6’ chain link fence with 3 horizontal strands of concertina wire on top. Approximately 80% of the north perimeter fence is covered by dense green plant and tree growth providing no clear zones and significantly impacting natural surveillance lines of site.

RECOMMENDATION: Maintain a clear zone on both sides of the fence by removing ground cover growth on and near the fence. Remove trees and or branches that may be used as a climbing aid and maintain all branch height at 12' or higher.

F. The facility is equipped with an exterior ladder which is not equipped with a lockable ladder guard to prohibit unauthorized access. This condition simplifies unauthorized access to the roof.
RECOMMENDATION:
Install a lockable ladder guard to mitigate unauthorized access.

1.2.5 Blending Station No. 2

Findings

A. Antiquated mercury vapor luminaires yield unwanted yellow glare into the video surveillance cameras.
RECOMMENDATION: Upgrade area lighting to motion-activated full-cutoff L.E.D. luminaires. For guidance on the selection of outdoor security lighting, see ANSI/ASCE/EWRI 56-10, Appendix 7.0.

B. The facility door has an exposed latch bolt and door hinges.
RECOMMENDATION: All perimeter doors should be equipped with protective metal latch-guards to restrict access. Ensure door hinges are properly pinned to prohibit removal from the exterior. Whenever possible, utilize internal door hinges, such as piano hinges, to minimize hinge tampering. See ANSI/ASCE/EWRI 56-10, Appendix 13.2 for door recommendations.

C. The 6' masonry block wall is easily scaled and is not equipped with any form of prohibitive fence topping similar to Blending Station No. 3 and 5.
RECOMMENDATION: Consider installation of fence topping on top of the masonry wall to reduce the trespassing exposure. For guidance on the selection of fencing topping, see ANSI/ASCE/EWRI 56-10, Appendix 1.5.

D. The perimeter masonry wall was not equipped with any signage.
RECOMMENDATION: See ANSI/ASCE/EWRI 56-10, Appendix 8.0, for perimeter signage recommendations.

1.2.6 Blending Station No. 3

Findings

A. All perimeter portals (vehicle and pedestrian) are operated by RFID access control system. Outside lighting is controlled and limits glare. Infrared cameras and motion detectors protect interior and exterior of buildings and monitor outside spaces and areas of importance, such as well pumps and chemical assets. Cameras are monitored by the Water Campus security office. A central station monitored intrusion detection system monitors the buildings during non-business hours.

B. Minimal signage was noted along the perimeter.
RECOMMENDATION: See ANSI/ASCE/EWRI 56-10, Appendix 8.0, for perimeter signage recommendations. No trespassing signage should be installed every 50.

C. An exterior door panic bar assembly (installed in the perimeter fence) is vulnerable to being opened from the outside.
RECOMMENDATION: Install protective panic bar flange over the panic bar to mitigate opportunities to open from the exterior.

D. The exterior motion detectors apparently were added to detect a determined adversary successfully scaling the fence.
RECOMMENDATION: A walk test of the exterior motion detectors should be conducted to ensure the existence of proper coverage patterns in relation to the core assets.

E. The facility doors have exposed latch bolts and door hinges.
RECOMMENDATION: All perimeter doors should be equipped with protective metal latch-guards to restrict access. Ensure door hinges are properly pinned to prohibit removal from the exterior. Whenever possible, utilize internal door hinges, such as piano hinges, to minimize hinge tampering. See ANSI/ASCE/EWRI 56-10, Appendix 13.2 for door recommendations.

F. Portions of the fence are covered with green ground cover growth which restricts natural surveillance lines of sight into the facility grounds.
RECOMMENDATION: Maintain a clear zone of the fence by removing ground cover growth on and near the fence. Remove trees and or branches that may be used as a climbing aid and maintain all branch height at 12’ or higher and maintain ground cover plants within the facility to under 36” high.

1.2.7 Blending Station No. 4

Findings

A. The 6’ masonry block wall is easily scaled and is not equipped with any form of prohibitive fence topping similar to Blending Station No. 3 and 5.
RECOMMENDATION: Consider installation of fence topping on top of the masonry wall to reduce the trespassing exposure. For guidance on the selection of fencing topping, see ANSI/ASCE/EWRI 56-10, Appendix 1.5.

B. The facility door has an exposed latch bolt and door hinges.
RECOMMENDATION: All perimeter doors should be equipped with protective metal latch-guards to restrict access. Ensure door hinges are properly pinned to prohibit removal from the exterior. Whenever possible, utilize internal door hinges, such as piano hinges, to minimize hinge tampering. See ANSI/ASCE/EWRI 56-10, Appendix 13.2 for door recommendations.

C. Minimal signage was noted along with perimeter walls.
RECOMMENDATION: See ANSI/ASCE/EWRI 56-10, Appendix 8.0, for perimeter signage recommendations. No trespassing signage should be installed every 50.

D. The building is not equipped with any form of intrusion detection or electronic access control.
RECOMMENDATION: Install an access control system with integrated intrusion detection in compliance with the PWIMP Security Concept of Design.

1.2.8 Blending Station No. 5

Findings

A. While in close proximity to the well-traveled Pleasant Valley Road, the set-back of the facility associated with curbing, thick shrubbery, and a substantial building structure, will likely prevent accidental or intentional vehicle intrusion to the front of the structure, but not necessarily to the western side or to infrastructure to the rear. The facility lies near the apex of a sweeping left bend in the roadway in addition to a dirt road to the south. Errant—or intoxicated—drivers could easily make an off-highway landing into the exposed rear portion of this station.

RECOMMENDATION: Install bollards or limiting devices to protect station from intentional or accidental intrusion from eastbound vehicles. Refer to ANSI/ASCE/EWRI 56-10, Appendix 5.0, for recommended bollard specifications.

A. Excellent perimeter fencing consisting of black, 6-foot ornamental aluminum fencing with anti-climb fencing topping is installed along the majority of the perimeter with the exception of a 6' masonry wall located on the eastside of the building. The wall is not equipped with any protective topping and may be easily scaled.
RECOMMENDATION: Consider installation of fence topping on top of the masonry wall to reduce the trespassing exposure. Fence companies such as Ameristar offer 3' high paneled fence toppings that may be installed on top of existing masonry walls. For further guidance on the selection of fencing topping, see ANSI/ASCE/EWRI 56-10, Appendix 1.5.

B. The card access controlled perimeter door is equipped with a glass window.
RECOMMENDATION: Apply Mylar burglary-resistant film secured in the frame (preferably) to minimize and delay forcible entry exposures. Consider darkest possible tint to minimize ability observe room assets from the outside looking in. Alternatively, consider a solid metal door replacement.

1.2.9 Well 27

Findings

A. No physical security measures are in place at Well 27.
RECOMMENDATION: Install a green colored PVC coated galvanized wire fence with 1" or smaller radius openings to minimize vandalism / tampering exposures.

1.2.10 Wastewater Lift Stations

Fifteen wastewater lift stations were identified by Public Works for assessment purposes.

Findings

A. While Lift Station 28 is protected by walls and has an on-site emergency power supply, and Lift Station 29 is monitored via a fixed surveillance camera due to its close proximity to a bus stop and 7-Eleven, most stations are located adjacent to roadways or in parking lots. A more likely scenario is an errant vehicle's impact into a lift station installed roadside or in a parking lot, either unintentionally or with criminal intent. The installation of bollards may be advisable at certain locations where traffic collisions are more likely to occur. Consultation with the city's traffic engineer would be appropriate. The widespread installation of bollards or other

vehicle impact mitigation strategies is not advised as such a program could easily cost more than any potential loss from an unintentional event involving a single wastewater lift station. RECOMMENDATION: Install bollards or other limiting devices as appropriate to protect lift stations from intentional or accidental intrusion from vehicles. Refer to ANSI/ASCE/EWRI 56-10, Appendix 5.0, for recommended bollard specifications.

1.2.12 Del Norte Regional Recycling & Transfer Station

Findings

A. Cash handling operations occur at several areas within the facility premise six days a week presenting an inherent potential robbery exposure.
RECOMMENDATION: Replace any non-ballistic rated glass within cash handling areas. Reinforce or replace doors, door frames, and locking mechanisms to resist forcible entry. Install concealed duress buttons monitored by a third party UL listed central station.

B. The facility metal doors have exposed latch bolt and door hinges.
RECOMMENDATION: All perimeter doors should be equipped with protective metal latch-guards to restrict access. Ensure door hinges are properly pinned to prohibit removal from the exterior. Whenever possible, utilize internal door hinges, such as piano hinges, to minimize hinge tampering. See ANSI/ASCE/EWRI 56-10, Appendix 13.2 for door recommendations.

C. Uncontrolled pedestrian accesses from the front parking lot into the interior collection area of the building is possible simply by walking just south of the Buy Back area and enter a narrow walkway where empty propane and oxygen tanks are stacked. This leads immediately to a single lane driveway for trucks entering into the southeast portion of the building. A pedestrian gate controlling access to the tank storage area may have been removed.
RECOMMENDATION: Take necessary measures to eliminate this security and general liability exposure.

1.2.13 Cathodic Protection Rectifiers

Findings

A. The installation of bollards may be advisable at certain locations where traffic collisions are more likely to occur. Consultation with the city's traffic engineer would be appropriate. The widespread installation of bollards or other vehicle impact mitigation strategies is not advised as such a program could easily cost more than any potential loss from an unintentional event involving a rectifier.
RECOMMENDATION: Install bollards or other limiting devices as appropriate to protect rectifiers from intentional or accidental intrusion from vehicles. Refer to ANSI/ASCE/EWRI 56-10, Appendix 5.0, for recommended bollard specifications.

APPENDIX B - PHYSICAL AND ELECTRONIC SECURITY BASIS OF DESIGN

CITY OF OXNARD

PUBLIC WORKS INTEGRATED MASTER PLAN

PHYSICAL AND ELECTRONIC SECURITY BASIS OF DESIGN

TABLE OF CONTENTS

APPENDICES

REFERENCES

This section of the report is intended to define the standards, criteria and assumptions used for the design, documentation and specification of physical and security systems. The security contractors will provide a written guarantee for a period of one year from the date of substantial completion that covers the entire system including equipment, materials and workmanship. The security system will comply with the following:

1. Guidelines for the Physical Security of Wastewater / Stormwater Utilities, ANSI/ASCE/EWRI 57-10
2. NFPA 730 (latest version) Guideline for Premises Security
3. NFPA 731 (latest version) Guideline for the Installation of Electronic Premises Security Systems
4. UL 1076 (latest version) Proprietary Burglar Alarm Units and Systems (When integrate with Access Control Systems, the Access Controls systems will meet this standard)
5. UL 294 (latest version) Access Control System Units
6. NEMA 250 (latest version) Enclosures for Electrical Equipment (1000 Volts Maximum)
7. NECA 1-2010 Standard Practice of Good Workmanship in Electrical Construction (ANSI)
8. NFPA 70 (2005) National Electrical Code

ABBREVIATIONS & ACRONYMS

ACS	Access Control System
AHJ	Authority Having Jurisdiction
A/E	Architect/Engineer
CBR	Chemical, Biological, and Radiological
CCTV	Closed Circuit Television
COO	City of Oxnard
COTR	Contracting Officer's Technical Representative
CPP	Certified Protection Professional
CPTED	Crime Prevention Through Environmental Design
DBT	Design Basis Threat
DGP	Data Gathering Panel
EMT	Electrical Metallic Tubing
ENT	Electrical Nonmetallic Tubing
ESS	Electronic Security System
FCC	Fire Command Center
IBC	International Building Code
OPW	City of Oxnard Public Works
SMS	Security Management System
SOC	Security Control Center
ULPA	Ultra Low Penetration Air
UPS	Uninterruptable Power Source

1 INTRODUCTION

The City of Oxnard, Public Works (OPW) Security Design Criteria are provided to architectural and engineering (A/E) design teams, security consultants, and OPW staff as guidance for the design and construction of OPW facilities. The design team shall utilize these criteria to the full extent when designing either new facilities or major renovations of owned or leased facilities.

This document provides design guidance for limiting or mitigating the risks associated with water and waste water property protection, common crime, terrorist attacks, or other manmade hazards. The guidance also provides some benefits for mitigating natural hazards. Guidance is provided for various aspects of planning and design. Design guidance is discussed and recommendations are given in each section for enhancing life safety and security.

This document should be used along with the latest versions of the Guidelines for the Physical Security of Wastewater / Stormwater Utilities, ANSI/ASCE/EWRI 57-10. Where conflicts occur, the design team shall immediately notify the Security Department (OPW) through the City of Oxnard, Public Works (OPW) Project Manager.

1.1 Purpose

This document defines the minimum security criteria required by the City of Oxnard Public Works, hereafter referred to as (OPW), owned and leased facilities and the spaces and assets within those facilities. This document was developed to ensure that security is consistently applied and becomes an integral part of the planning, design, and construction of all projects within OPW. The criteria considers security in all building systems and elements.

The objective of this manual is to a provide cost effective design criteria that provides the appropriate level of security protection to the facility.

1.2 Applicability

This OPW Security Design Criteria is applicable to all OPW facilities under their responsibility, including leased facilities. The primary objective of this manual is to provide the design team and OPW staff with consistent criteria and standards for existing and new buildings. It is intended to supplement other OPW design guidance.

These standards apply to new construction and all additions, alterations, and modernizations. These standards apply to only the spaces being renovated in an existing building, and do not extend to other spaces in the same building except as may be directed by OPD. Existing facilities not undergoing any renovation will be brought up to compliance through separate security projects sponsored by OPD.

The criteria used in this document are based on risks common to water and waste water properties, and offices are consistent with other standards developed for these types of facilities (See References). Additionally, this document recognizes that risks are unique to each facility and the assets that they may house. Therefore, the criteria developed also vary by facility type, space usage, and risk categorization.

1.3 Authority

City of Oxnard, Department of Public Works Security Operations Policy _____, dated _____. [a policy document should be developed providing authority of this document as a requirement for design and construction department.]

1.4 Using this Document

The document is divided into chapters, each of which represent a design disciplines of conventional architectural and engineering teams, which include architecture, civil, mechanical, structural, etc. and potentially specialty consults for special systems including fire protection and electronic security systems.

Security is often viewed as layers of protection from the most unsecured layer (beyond the perimeter) to the most secure layer often securing our assets (see figure 1, Layered Security Design). Some examples of most secured assets are data centers, water storage, water treatment systems and materials, utilities, and people.

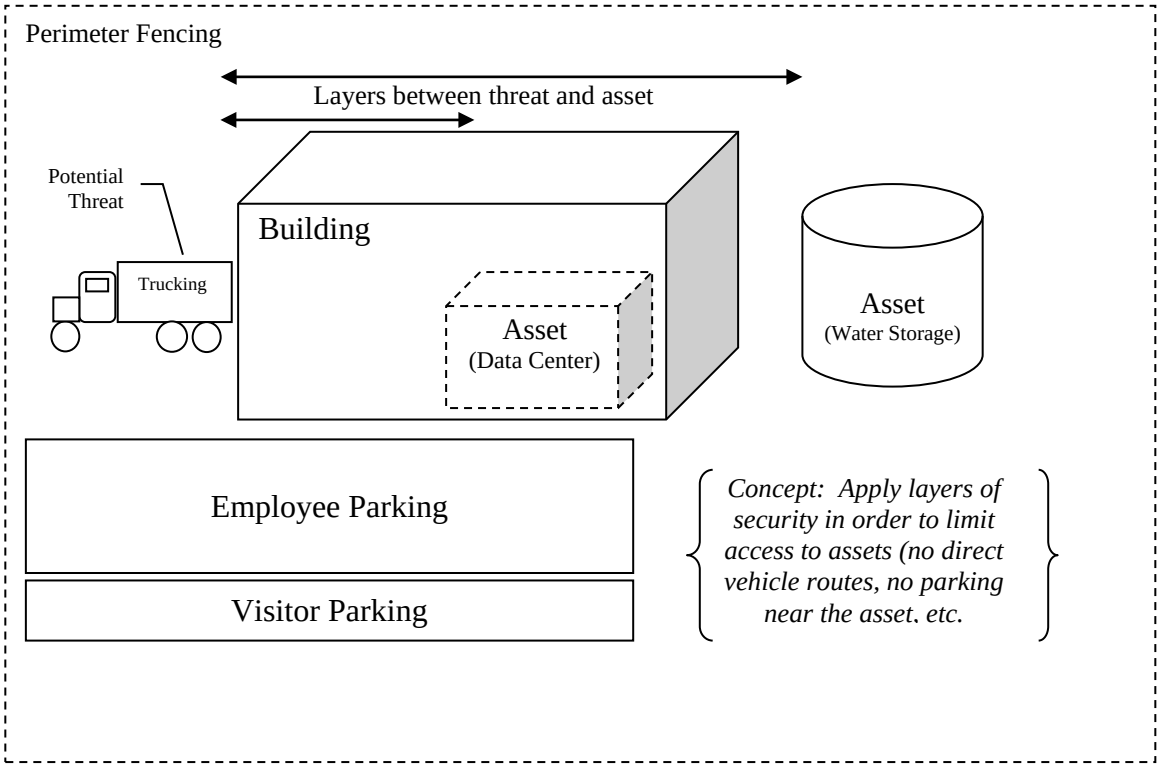


Figure 1: Layered Security Design

Layers of protection (security layers) are often applied in various approaches, however the main concept is to apply layers of security necessary to protect the asset. In general concept assets can be people (staff and public), places (water treatment, wells, etc.) or things (water, money, pumps, water treatment materials, etc.) that need to be protected. It is important that layers are applied correctly to protect the asset. For instance, if the threat is criminal activity of stealing data from the datacenter; card readers and cameras at several layers (site, building, staff only areas, and data center) will help control access to the asset assuming the threat is not an insider that works in the data center. Therefore an additional measure may be protecting specific data from access to employees (who don't need to access it) and provide background checks and other controls to restrict access. However, that approach may not be appropriate for another threat such as sabotage of water resource, where the counter measures may be similar, but the tactics may be different. For that reason, baseline security measures are often sought to provide basic levels of security (fencing, lighting, signage, cameras, etc.); while more specific countermeasures focus on individual threats types and tactics. It is known that baseline

strategies are common to protect or deter a group of low level threats, therefore most practitioners apply a baseline approach (i.e., all water storage facilities in the United States have security fencing, vehicle controls, lighting). Then, based on a risk assessment, apply enhanced measures to counter specific threats. An enhanced approach would be to provide more active systems such as card reader systems, cameras and guard forces to control access to the water resource. This concept is applied in the master plan.

Other than Chapter 2, each chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria.* The protective measures identified in this document generally are intended for threats associated with water and waste water property protection, and crime office and workplace violence. For threats associated with domestic or international terrorism, where appropriate, the user is directed to the *Guidelines for Physical Security of Water Utilities and Guidelines for the Physical Security of Wastewater/ Storm water Utilities (ANSI/ASCE/EWRI 56-10 & 57-10)* for guidance. Implementation of these guidelines requires an individual facility risk assessment. User's should obtain the referenced guidelines from their codes and standards providing organization.

- **Best Practices** are encouraged design considerations, but some or all considerations may not be practical for every project. Designers should strive to meet Best Practice requirements where feasible.
- **General "Baseline" (Minimum) Criteria** are OPW requirements which must be met in all projects. General Criteria provide specific information on the application of criteria for all spaces.
- **Threat Based "Enhanced" Criteria** are OPW requirements which must be met in all projects. The Site and Space Specific Criteria identifies performance based measures that are to be applied by site and facility type based on a specific design basis threat assessment. The Enhanced Security Measures in **Appendix A** of this document, identifies the appropriate risked based measures arranged by ***Site and Perimeter***, ***Facility Structures, Power and Wiring, Video Surveillance and Perimeter and Intrusion Detection***. To use the matrix select the facility type listed in the left-hand column of the table then locate the measures under each category. The categories are consistent with the OPW facility types. Go to the paragraph listed in this document to determine the measures for each facility. The criteria listed in the Security Matrix are the minimum acceptable for each space. In some instances, outside factors will require the baseline criteria be augmented or supplemented. Only OPW can approve any modifications to the design criteria for a facility or space. If the security requirements can be defined by two different "facility types" (i.e. personnel offices within the perimeter of the water treatment facility), the more stringent requirement shall be applied.

1.4.1 New Construction / Major Modernization vs. Existing Construction

This document recognizes that not all physical security measures can be reasonably implemented on existing facilities unless they are undergoing a major renovation. Therefore, the Enhanced Security in Appendix A categorizes the measures for each space and discipline into two categories; Existing and New Facilities. In some disciplines (i.e. electronic security, fencing) the measures are relatively the same for both existing and new facilities. However, other disciplines (i.e., major wall construction or locations within the Architecture chapter) have different measures for the two

categories. This is intended not to overly burden projects with requirements that may be unreasonable based on their scope. However, project managers and planners should consider integrating facility requirements if it is found that security deficiencies must be mitigated in a future project. In all cases, major renovations and new construction must meet the requirements of this document.

1.4.2 Measure Substitution

Where possible, the criteria have been written in a performance based format in order to provide the designer or user the most latitude in determining the best overall solution for OPW. Where prescriptive criteria have been used, the designer may recommend alternative solutions with justifications to OPW for consideration.

1.4.3 Design Deliverables

Appendixes B, C & D provide additional guidance (beyond the OPW Design Management Guide) for the design of electronic security systems. Appendix B provides information and guidance on the type of drawings required by OPW to document the Electronic Security System, including the drawings required in the various design submission as well as the level of detail expected at each. Appendix C provides standard drawings to demonstrate the level of detail required by OPW. Appendix D is an outline specification for the Electronic Security Systems.

1.5 References

The identified references used to develop this document contain both best practices and minimum criteria. The identified additional references are tools for the design team to use to implement the best practices and minimum criteria established by this document.

1.6 Construction Specifications

The OPW Construction Specifications for Electronic Security provide specific guidance for the installation of ESS components and complete systems in order to ensure uniform results across the enterprise. While this document provide general guidance, project specific specifications for electronic security should be developed This guidance defines installation methods, materials, and procedures.

2 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

The City of Oxnard Public Works (OPW) advocates the integration of Crime Prevention Through Environmental Design (CPTED) principals and strategies in their site planning and facility designs. CPTED principles and techniques seek to create a physical and operational environment which discourages criminal or other wrongdoer activity by incorporating territorial cues, natural access controls, and natural surveillance. As discussed in the assessment portion of our work, CPTED should be used for all facilities using a variety of techniques to assure consistent results no matter the facility type.

2.1 Crime Prevention Model

The model for crime prevention through environmental design is based on the theory that action must be taken to counter crime or wrongdoer activity before it occurs. The critical element in this model is the environmental-engineering component. It provides both direct and indirect controls against criminal or other wrongdoer activity by reducing the opportunity for criminal or terrorist activity through the use of science and technology and various urban planning and design techniques. The model explains what environmental engineering is and how it supports crime or wrongdoer prevention. With this information, the design team may be in a better position to understand and respond to questions and discussions on how site and facility planning can have an impact on criminal or other wrongdoer elements.

2.2 The Environmental Influence on Criminal Behavior

The basic theory that supports crime prevention through environmental design is that urban environments can influence criminal behavior in two ways.

- First, the physical surroundings in which people live have an effect on each individual. These physical characteristics include noise, pollution, overcrowding, and the existence and unmonitored spreading of refuse and other unsightly waste.
- The second element which must be dealt with in the environmental-engineering formula concerns the social characteristics of the site that provide individuals with social relationships to which they must respond. Characteristics such as alienation, loneliness, anxiety, and dehumanization are seen as keys to criminal behavior.

In terms of these environmental characteristics, buildings are all too often constructed to be dangerous, with corridors and passageways or facilities hidden from public view. Elements such as opaque fencing, insufficient lighting, facility maintenance debris, unsecured storage facilities, and even basements and janitor closets are also laden with danger due to their design.

With regard to altering the social characteristics of the area (OPW water and waste water facilities, water transport and offices) and the relationship to wrongdoer behavior, it should be recognized that behavior is future-oriented, not past-oriented. A person steals so that they can have a car or money in the future, not because in the past he experienced psychic trauma, a broken home, poverty, or delinquent associates. Criminal behavior can be explained directly in terms of the consequences of behavior and in terms of non-criminal variables such as poverty, race, or social class. Criminal behavior is viewed as a problem to be dealt with and not a symptom of other problems (such as poverty, mental conflict, class conflict, unemployment, or under education). Terror, while linked directly to group political, religious or other ideological beliefs; most targets are attacked due to their attractiveness including how soft the target is. Soft target is a sense of the criminal or aggressor to succeed in carrying out their act due to ease of the act on the given facility and reward the acts impact (i.e., contaminate the water supply effecting the population,

theft of materials to support carrying out another act, vandalizing a facility without getting caught). To change this behavior or even reduce the impact, it must be dealt with directly by removing the environmental reinforcement which maintains the behavior. The approach advocated is to change the environment to which the individual responds. Three overarching CPTED principles are used Territorial Reinforcement, Natural Surveillance, and Natural Access Control.

2.3 Territorial Reinforcement

Historically, a building on its own piece of land and somewhat isolated from its neighboring buildings (but often by as little as a few feet) has been considered to be the building's territory. The building sits on a piece of land buffered from neighbors and the public street by intervening grounds. At times, symbolic shrubs or fences reinforce a boundary. The positioning of lights to look out on the grounds and good natural surveillance act to reinforce the territorial claim. Other elements include warning signs, or signage identifying OPW property. A number of concepts have been identified which may be used in new construction or renovation projects.

- Define property lines. Even a small picket fence in the front yard does this psychologically. Driveway and sidewalk pigmentation color changes may be used.
- Use landscaping to designate areas which are off limits.
- Design pathways, gates, or signs to emphasize the differences between spaces.
- Use security lighting or security systems to establish boundaries.
- Have customers walk past a "checkpoint" staffed by a person or camera.
- Display security signage at access points.

These mechanisms encourage the building staff and other tenants to identify more with the ground or area around their immediate site and to assume responsibility for its protection.

2.4 Natural Surveillance

Experience has shown the ability to observe criminal or other wrongdoer activity may not be adequate to stimulate an observer to respond with assistance to the person or property being victimized. The decision to act depends on the presence of motivational conditions, including:

- Windows overlooking sidewalks and parking lots.
- Security lighting in strategic locations at night.
- Low cubicle office space dividers in office bull pen environments
- Open stairways and elevators.
- Maze entrances in commercial buildings, thus eliminating doors.
- Keeping windows of commercial establishments free of excess signage or obstructions.
- Placing work and leisure activities in the open where people see each other.
- Compliment Natural Surveillance measures with security cameras and signage.

The benefit or output of these examples provides:

- the degree to which the observer has developed a sense of personal and property (ownership like) rights which may or will be violated by the criminal act,

- the degree to which the observer feels the event is within their area of influence,
- the observer's ability to clearly identify whether the act is unusual for the particular area,
- the observer's identification with either the victim or the property being vandalized, and
- the degree to which the observer believes he/she can effectively alter the course of events they are observing.

2.5 Natural Access Controls

Natural Access Control is meant to control or limit the opportunity for crime by clearly defining the differences between public and private spaces. By selectively placing entrances and exits, fences, lighting, and landscaping, you can limit access, or control the flow of people to better manage this concept. Denying access to crime targets can deter criminal activity by creating a perceptual risk to aggressors. Natural Access Control planning can reduce the need for expensive security equipment. Here are some examples of Natural Access Control.

- Highlight the main entrance to a building.
- Clearly mark public walkways and paths.
- Use landscaping to encourage use of public walkways and pathways and discourage access to off-limits areas.
- Clearly identify areas that are off-limits to the public.
- Design streets and sidewalks to physically guide people where you want them.
- Design or construct see-through fences.
- Limit the number of entrances and exits to buildings and even parking lots.

Design features that clearly indicate public routes and discourage access to private structural elements. These features decrease an opportunity for crime by creating in an offender a perception of unacceptable risk when attempting access to private areas, which marks the stranger as a possible intruder. Such design features include placement of entrances and exits, fencing, and landscaping to control traffic flow.

2.6 Defensible Space

Defensible space is a term for a range of combined security measures which brings an environment (i.e., territoriality, natural access controls, technology, procedures) more under the control of its owners, operators, staff and/or residents. A defensible space is a building environment which can be used by inhabitants for the enhancement of their lives while providing security for themselves, coworkers, and visitors. Examples of effective defensible space:

- Utility areas discouraged a criminal from accessing the site because they felt the likeliness that they would be caught was high.
- Aggressor selects an alternate site than Oxnard's Public Utility, because the target was hardened and difficult to assure a successful attack. In this case, the aggressor (during pre-attack planning) sees that personnel are keenly aware of their presence, and site improvements cause concern to the aggressor that their attack would not be achieved.

- OPW maintenance personnel identify, report and police later apprehend suspicious man attempting to load chemicals into a treated water connection point. In this instance, good site surveillance improvements caused the aggressor to be seen early in the attempt to contaminate water infrastructure.

The physical concepts suggested to create safety and improve upkeep (as part of the defensible-space concept) are self-help tools wherein design catalyzes the natural impulses of staff rather than forcing them to surrender their shared social responsibilities to any formal authority.

2.7 Action Planning for Crime Prevention Through Physical Planning

Many organization's security and police activities have become involved in the physical-planning process and have achieved notable results from their work. This involvement includes evaluating the accessibility of buildings and locations of security patrols and posts; pedestrian and vehicle traffic flow; and off-street parking provisions; and the layout and adjacencies of access roads, garden areas, utility areas (e.g., generators, transformers, water utilities, communications hubs, boilers and chillers), common greens, fences, and entrances. There are a number of concerns to OPW that should be carefully examined from a security perspective. Some examples of specific concerns:

- Building setbacks (front, side, and rear). Includes reduction or elimination of crevasses around building, interior spaces, and landscaping.
- Wall construction, interior and exterior (industrial, commercial, and residential).
- Door construction, building setback and security (industrial, commercial, and residential) including carports, garages, and sliding-glass doors.
- Windows and skylights, building setback, window height (from ground), show-window displays, and the type of frame or pane.
- Fences, walls, hedges, screens, building setback, building height, and louvers.
- Parking (public and private) away from assets.
- Lighting for site lighting around walkways, entrances, vehicle access-ways and critical assets.
- Streets, sidewalks, and walkways (locations, slopes, curvature, grades, and the length of a block). When practical eliminate crevasses or hiding areas by smoothing curves and slopes away from walkways.
- Alleys and crevasses (hiding places) are well lighted and clear of obstacles. Designs should eliminate alleys and crevasses where practical.
- Visibility of assets (people, utilities, and materials and equipment) should be maintained.
- Signs (street signs and signals, no trespassing signs, traffic signs and signals, and advertising signs).
- Accessibility; approach, entrance, and exit (pedestrian, vehicular, services, residential, commercial, and industrial).
- Funnel access to areas with increased surveillance (natural, line of sights, CCTV)
- Design a layered system of security considering environmental, physical including electronic and operational security elements; planned high risk assets on most secured (internal) layers

- Minimize concealment opportunities in landscaping and street furniture, such as large thick hedges, trees with low branches, bus shelters, grass heights, benches, and trash receptacles
- Establish setbacks of approximately 20 feet; all perimeter fences and walls secured; and free of trees, debris or structures that can be used to climb
- Define primary entrances for access and define any other entries so that all public access is controlled in one point; egress should be funneled to select egress points (emergency egress should be planned in concert with egress plans);
- Control room for security and environmental monitoring with CCTV, access checkpoints, and intrusion circuits
- Avoid opaque fencing and landscaping that might provide hiding spaces and limit surveillance
- Design circulation to minimize speeds of vehicles and eliminate direct approach conditions
- Incorporate vehicle barriers into site design; such as, walls, fences, trees
- Locate critical offices and assets away from public spaces

2.8 Design Team Guidance

The City of Oxnard, Public Works (OPW) encourages design teams to explore these CPTED concepts and principles in their projects. To encourage a multi-disciplinary approach to CPTED, 'discipline specific strategies' are introduced in the following chapters to assist designers in addressing security concerns. These strategies help prepare the design team in understanding CPTED and support its benefits in OPW facility designs.

3 SITE LAYOUT

This section discusses site-level considerations for development. The intent of this guidance is to provide concepts for integrating land use planning, landscape architecture (vegetation, landforms, and water), site planning, and other strategies to mitigate the design basis threats as identified by OPW via the risk assessment. Integrating security requirements into a larger, more comprehensive approach necessitates achieving a balance among many objectives such as reducing risk; facilitating proper building function; aesthetics and matching architecture; hardening of physical structures beyond required building codes and standards; and maximizing the use of non-structural systems.

The design team must work closely with building owners and operators to ensure the optimal balance of all the above considerations is achieved; thus, coordination within the design team is critical. Many asset protection objectives can be achieved during the early stages of the design process when mitigation is the least costly and most easily implemented. Planners, architects, landscape designers and security consultants play an important role in identifying and implementing crucial asset protection measures while considering land use; site selection; the orientation of buildings on the site; and the integration of vehicle access control points, physical barriers, landscaping, parking, and the protection of utilities to mitigate threats.

This chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria*. Best Practices are encouraged design considerations, but some or all considerations may be impractical for the project. General Criteria and Space Specific Criteria are OPW requirements which must be met in the project design.

3.1 Principle Best Practice

The design team is encouraged to utilize the following best practices when determining the appropriate and cost-effective measures for incorporation into the building and site design.

3.1.1 Site Design

Because the economics of development dictate recovering the largest possible portion of square footage within most urban and rural sites, security concerns should be evaluated carefully. Conflicts sometimes arise between security site design and conventional site design. To maximize safety, security, and sustainability; designers should implement a holistic approach to site design which integrates form and function to achieve a balance among the various design elements and objectives. Even if resources are limited, significant value can be added to a project by integrating security considerations into the more traditional design tasks in such a way that they complement, rather than compete with, the other elements.

The overall layout of a site (e.g. the placement and form of its buildings, infrastructures, and amenities) is the starting point for this integration. Choices made during this stage of the design process will steer decision-making for the other elements of the site. A number of aspects of site layout and building type present security considerations and are discussed below.

a. Building Placement

The ideal building placement from a security standpoint incorporates the three basic CPTED principles of Territorial Reinforcement, Natural Surveillance and Defensible Space. Some general guidelines for incorporating each element are discussed below.

1. Territorial Reinforcement
   a) Site Design

      If the grounds around a set of buildings or structure can be directly identified with a particular building where building occupants play a role in protecting it, then strangers are usually recognized and their activities come under observation and immediate questioning. Even in public areas like OPW water treatment, wells, cross connects, purification facilities; strangers with wrongdoer intent are noticed, questioned, and placed under surveillance (either by staff or by security personnel).

      The placement of the building should provide territorial reinforcement of the ownership by creating a distinction between the public domain and that of the building. This can be accomplished through the use of clear space to separate the two entities.

   b) Street and Access Road Design

      Research has shown that the placement, enclosure, or routing of roadways and traffic can change the nature of a particular area and reduce wrongdoer activity. For example, a particular portion of a street might be closed to vehicular traffic (near assets like storage facilities), and streetscape equipment (vegetation, lighting, fencing, etc.) may be added to define territory.

      In a number of areas where this technique has been utilized, it has been found that most people know or at least recognize other people up and down the block and suspicious activity on the street is identified. Similar approaches which involve rerouting traffic away from most critical operations, or equipment and providing access controls such as gates and vehicle control systems, using one-way streets, or blocking off streets has reduced wrongdoer activity.

   c) Symbolic Barriers

      The types of barriers that planners may use when laying out an area include open gateways, light standards, low walls, earth berms, and plantings. Both physical and symbolic barriers serve the same purpose—to inform an individual that he/she is passing from a public to private space. Wrongdoers sense they are traversing from one area to another when barriers are in place. Symbolic barriers identified by people as boundary lines serve as defining areas of comparative safety. Many places warrant the use of symbolic barriers, including transition points between a public street and the semi-public grounds of a building; an area between a building's lobby and its corridors; or hallways on particular floors of a building.

2. Natural Surveillance

   That same clear space aides the natural surveillance, increasing the risk to individuals desiring surreptitious entry to the facility. The building should be oriented in order to eliminate or at least minimize areas which cannot be seen by a casual observer.

3. Natural Access Controls

   Provide visual and physical cues to funnel vehicles and pedestrians towards public space where interaction with facilities personnel is planned, and funnel

them away from the assets that are critical or vulnerable. Well placed access controls also support natural surveillance and highlight when wrong doers are driving and walking against the access controls in place (ultimately triggering staff and security to notice something is not right).

4. Defensible Space

   The clear zone also provides defensible space by providing the opportunity to have several layers of security before entering the building. For instance, defining the site through territorial reinforcement is one layer, the natural surveillance is a second layer, and the building façade is yet another layer. The clear space also provides standoff distance which will be discussed further.

   Research has revealed investigative techniques that may be used to modify existing building areas to make them more secure. The following methods may require alteration or adaptation to the particular situation on your design project:

   - Widening major pathways and using colored decorative paving.
   - Differentiating small private areas (maintenance yards, water treatment equipment, etc.) outside each building or structure from the public path with low, symbolic walls.
   - Adding new lighting to highlight various paths at night and extending the occupants' surveillance potential and feeling of security.
   - Redesigning parking around buildings to create the illusion the buildings are grouped where natural surveillance opportunities exist.

b. Building Orientation

The orientation of a building or other structures can have a significant impact on its performance, not only in terms of energy efficiency, but also in the ability to protect occupants or other assets. For this document, the term "orientation" refers only to the building or structure's spatial relationship to the site. A structure's orientation relative to its surroundings defines its relationship to that area. The physical positioning of a building or structure relative to its surroundings may seem subtle, but can be a greater determinant of this intangible quality than exterior aesthetics.

For example, the proximity of a vulnerable façade to a parking area, street, adjacent site, or other area which is accessible to vehicles and/or difficult to observe can greatly contribute to its vulnerability. A strong, blank wall with no glazing will help to protect the people, property, and operations within from a blast, but the lack of windows limits the opportunities for natural surveillance of activities outside. Designers should consider such trade-offs early in the design process, in an effort to determine an acceptable level of risk. The same approach applies to siting any structure or utility element.

3.1.2 Standoff Distance

Standoff distance is the distance between an asset and a threat. Blast energy decreases as the inverse of the cube of the distance from the position of the explosion, therefore every additional increment of distance provides increasingly more protection. There is no ideal standoff distance; it is determined by the type of threat, the type of construction, and the desired level of protection. When planning, attempt to achieve the highest reasonable standoff practical.

The primary design strategy is to keep threats away from inhabited buildings. Although sufficient standoff distance is not always possible in conventional construction,

maximizing the distance may be the most cost-effective solution. Maximizing standoff distance also ensures there is opportunity in the future to upgrade buildings or structures to meet increased threats or to accommodate higher levels of protection. Stand-off distance must be coupled with appropriate building hardening to provide the necessary level of protection to assets.

One method to attain the appropriate level of protection and ensure stand-off distance between assets and potential threats is with the creation of controlled access zones. These zones attempt to limit access to the area immediately surrounding a building or structure. Although a controlled access zone is one of the best methods of providing standoff, such issues as site limitations, building placement, and property line restrictions do not always allow this zone to be created.

The standoff distance can be separated into two distinct zones known as the exclusive zone and the nonexclusive zone. The standoff distance for each zone should be determined based upon the Design Threat Level found in *Guidelines for Physical Security of Water Utilities and Guidelines for the Physical Security of Wastewater/ Storm water Utilities (ANSI/ASCE/EWRI 56-10 & 57-10)*

3.1.3 Circulation

The movement of people and materials into, through, and out of a site or facility is determined by the design of its circulation system. This system should be designed to maximize efficiency while minimizing conflicts between vehicles and pedestrians. Designers should begin with an understanding of the site's transportation requirements based on an analysis of how the facility will be utilized. This includes the parking volume necessary, pedestrian patterns and the modes of transportation they will use, and the number and types of access points required. Several aspects of transportation planning can impact security and are discussed below.

c. Parking

There are three primary types of parking facilities, all of which present security trade-offs. Surface lots can be designed to keep vehicles away from buildings, but they consume large amounts of land. They can also be hazardous for pedestrians if dedicated pedestrian pathways are not provided. In contrast, on-street parking is often convenient for users but this type of parking may provide little or no setback. Finally, garage structures can provide revenue and be convenient for users, but they may require structural measures to ensure blast resistance as well as crime prevention measures to prevent street crime. Although the cost of land suggests the construction of a garage below a building may be the most economically viable approach for many developments, they can be highly vulnerable to vehicle-borne weapons, endangering the building above. If garages must be used, additional security measures will be necessary to ensure safety.

Parking restrictions can help keep potential threats away from a building. In urban settings, however, curbside or underground parking is often necessary and sometimes difficult to control. Mitigating the risks associated with parking requires creative design measures, including parking restrictions, perimeter buffer zones, barriers, structural hardening, and other architectural and engineering solutions. Operational measures may also be necessary to inspect or screen vehicles entering parking garages. Reference the OPW provided risk assessment to determine if vehicle delivered bombs are a concern for the facility under design. If so, users must seek assessment and design guidance and requirements for parking, circulation, and other site access considerations.

d. Signage

Way finding is an important function of design which illustrates the importance of coordination among practitioners and community planning, public works, transportation, law enforcement, and fire-rescue organizations. The ability of users to navigate an unfamiliar environment is important for its success on a day-to-day basis, but will become critical in an emergency situation. In addition to overt prompts such as landmarks, architectural elements, and clear, consistent signage and maps, users will subconsciously rely on cues from their surroundings to help them select a path to safety. Similarly, emergency responders will depend in part on these design elements in order to navigate the scene.

Signs are an important element of security. Confusion over site circulation, parking, and entrance locations can contribute to a loss of site security. Signs should be provided off site and at entrances. There should be on-site directional, parking, and cautionary signs for visitors, employees, service vehicles, and pedestrians. Unless required, signs should not identify sensitive areas.

3.1.4 Lighting

Lighting shall provide for safety and security without compromising the quality of the site, the environment (including neighboring properties), or the architectural character of the buildings. The following are the basic lighting design criteria.

a. Aesthetics.

The site lighting shall provide desired illumination and enhancement of trees, landscaping, and buildings without providing dark shadowy areas compromising safety and security.

b. Pathways.

Pedestrian and bicycle pathways and walks, including bike racks, gates, and other features shall be illuminated in support of video and visual surveillance while providing for safety without objectionable spill onto adjacent areas on and off site.

Consider LED lighting where practical. All lighting should consider effects on Dark Skies initiatives.

3.1.5 Infrastructures and Lifelines

Providing power, gas, water, wastewater, and communications services is one of the most basic requirements project site. At the site scale, all critical lifelines should have at least one layer of redundancy, or backup. By eliminating single-point vulnerabilities, designers reduce the chance that service will be interrupted either intentionally or unintentionally. It is important to note that collocating a backup lifeline with its primary lifeline does not eliminate single-point vulnerability; only physical separation can substantially increase the likelihood of continuity of service. Designers should be aware that this could create the need for each type of infrastructure lifeline to cross the site perimeter at multiple locations, potentially complicating the process of managing utility easements and rights- of-way. Additionally, all controls, interconnections, exposed lines, and other vulnerable elements of infrastructure systems should be protected from access and exploitation by surveillance and/or physical countermeasures.

To minimize the possibility of such hazards, apply the following measures:

- Where possible, provide underground, concealed, and protected utilities.

- Provide redundant utility systems to support site security, life safety, and rescue functions.
- Prepare vulnerability assessments for all utility services to the site, including all utility lines, storm sewers, gas transmission lines, electricity transmission lines, and other utilities which may cross the site perimeter.
- Locate petroleum, oil, and lubricant storage tanks and operations buildings at lower elevations from all other buildings. Locate fuel storage tanks at least 30.5 m (100 ft) from buildings.
- Locate the main fuel storage away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).
- Provide utility systems with redundant or loop service, particularly in the case of electrical systems. Where more than one source or service is not currently available, provisions should be made for future connections. In the interim, consider "quick connects" at the building for portable backup systems.
- Place trash receptacles as far away from the building as possible; trash receptacles should not be placed within 9 m (30 ft) of a building.
- Locate utility systems at least 15.25 m (50 ft) from loading docks, front entrances, and parking areas.
- Manhole covers 25.4 cm (10 in) or more in diameter must be secured to prevent unauthorized opening. They may be secured with locks and hasps, by welding them shut, or by bolting them to their frame. Ensure hasps, locks, and bolts are made of materials that resist corrosion. Keyed bolts (which make removal by unauthorized personnel more difficult) are also available.

3.1.6 Landscape and Urban Design

For the purposes of this document, these two domains are virtually overlapping and will therefore be addressed together.

a. Landscape Design.

The implications of security for landscape design affect everything from plant species and building material selection to landform construction and way finding. Elements such as landforms, water features, and vegetation are among the building blocks of attractive and welcoming spaces, and they can also be powerful tools for enhancing security. These features can be used not only to define or designate a space, but also to deter or prevent hostile surveillance and unauthorized access. However, landscaping can also have detrimental impacts for safety and security, and practitioners should consider the unique requirements of the project to ensure the landscape design elements they choose will be appropriate and effective.

With careful selection, placement, and maintenance, landscape elements can provide visual screening which protects sensitive operations, gathering areas, and other activities from surveillance without creating concealment for covert activity. However, dense vegetation in close proximity to a building can screen illicit activity and should be avoided. In clear zones, vegetation should be selected and maintained with eliminating concealment opportunities in mind. Similarly, measures to screen visually detractive components such as transformers, trash compactors, and condensing units should be designed to minimize concealment opportunities for people and weapons. When developing landscape designs, ensure the long-term

growth plan is evaluated to ensure vegetation will not interfere with natural surveillance, create hiding spots, or interfere with CCTV cameras and lighting.

b. Urban Design

Through urban design, practitioners seek to create vibrant, inviting, and functional places for people to live, work, and play. To protect people, property, and operations, and to reduce liability, security should be considered a necessary aspect of these characteristics. If people do not feel safe, they will not use a place and, if a place is not used as intended, it will fail to fulfill its purpose. This failure can, in turn, result in a net loss to the community in terms of social, economic, and environmental sustainability.

Numerous urban design elements present opportunities to provide security. The scale of the streetscape should be appropriate to its primary users, and it can be manipulated to increase the comfort level of desired users while creating a less inviting atmosphere for users with malicious intent. However, even at the pedestrian scale, certain operational requirements must be accommodated. For example, although efficient pedestrian and vehicle circulation systems are important for day-to-day living, they are also critical for emergency response, evacuation, and egress. Furthermore, despite an emphasis on downsizing the scale of the streetscape, it is critical to maintain the maximum stand-off distance possible between vehicles and structures.

At the site perimeter, walls and fences used for space definition may be hardened to resist the impact of an explosive-laden truck; however, planters, bollards, or decorative boulders could accomplish the same objective in a much more aesthetically pleasing manner. Such an approach also creates permeability, which would allow pedestrians and cyclists to move more easily through the space.

Similarly, street furniture (e.g., mailboxes, bus stop shelters, light poles, works of art, street trees, planters, bicycle racks, seating, newspaper boxes, kiosks, and trash receptacles) can be used to enhance security. For example, bus stop shelters can be designed to allow for easy surveillance and detection of suspicious activity and objects. Hardened versions of everyday items, such as light poles, planters, benches, street trees (of appropriate size and type), and even water fountains can serve as vehicle barriers. These items maintain stand-off while creating a line of protection that is virtually transparent and highly permeable at the pedestrian scale. Note that in-ground installation of bollards, fences, and any other anti-ram measures should be preceded by an assessment of soil conditions and underground utilities in the immediate vicinity.

A main challenge for the design community is to reach the desired level of protection without turning the building or facility into a bunker or fortress. In other words, they are required to incorporate subtle and aesthetically pleasing security measures when involved in urban design projects. Below are some rules of thumb which should be taken into consideration when designing an urban landscape with a security component:

- Security measures must not impede access to public entrances or pedestrian flow on adjacent sidewalks.
- Landscape elements in the form of grassed plinths, trees, plantings, fountains, and pools are appropriate, but must be designed as integral parts of a building and its setting as much as possible.

- Miscellaneous decorative elements such as flag poles, fountains, pools, gardens, and similar features may be located within an access path to slow movement or restrict access.
- Trees planted along the inside edge of a public sidewalk and adjacent to pedestrian and vehicular paths can serve dual aesthetic and barrier purposes.
- The design of bollards, fences, light posts, and other streetscape and landscape elements should form an urban ensemble which helps to create a sense of unity and character.
- Security devices must be designed and located to establish consistent, rhythmic patterns along the street, particularly where a number of elements are used in combination to reduce visual street clutter.

3.2 General Criteria (Baseline Requirements)

General criteria are baseline requirements that will be implemented. Where measures are deemed impractical due to environmental limitations or funding, consider operational measures that can be implemented. Where baseline measures are not met, a risk measure acceptance should be documented.

	Raw Water		**Wells & Pumping**		**Water Treatment**		**Finished Water Storage**		**Water Distribution**		**Water System Support**	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
Assess and Deploy CPTED principles	●	●	●	●	●	●	●	●	●	●	●	●
Site circulation should limit access to assets	BP	●	BP	●	●	●	●	●	BP	●	●	●
Basic perimeter fencing or perimeter walls	●	●	●	●	●	●	●	●	●	●	●	●
Foundation enhancements to prevent tunneling	●	●	●	●	●	●	●	●	●	●	●	●
Key operated gates	●	●	●	●	●	●	●	●	●	●	●	●
Perimeter lighting	●	●	●	●	●	●	●	●	●	●	●	●
Gate entrance lighting	●	●	●	●	●	●	●	●	●	●	●	●
Harden site openings larger than 96 in^2 (e.g., grates on culverts)	●	●	●	●	●	●	●	●	●	●	●	●
"No Trespassing" signage (every 50 ft)	●	●	●	●	●	●	●	●	●	●	●	●
Motion activated lighting	BP	●		●	●	●	●	●		●	●	●
Perimeter minimum clear zone distance	WP	●	WP	●	WP	●	WP	●	WP	●	WP	●
Chemical storage and feed equipment (outdoor) locked access					●	●					WP	WP
Landscaping does not obscure building or other assets	●	●	●	●	●	●	●	●	●	●	●	●
Manholes –locked with security fastener	●	●	●	●	●	●	●	●	●	●	●	●

	Raw Water		Wells & Pumping		Water Treatment		Finished Water Storage		Water Distribution		Water System Support	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
Minimize exterior signage indicating the presence of, type or locations of assets	●	●	●	●	●	●	●	●	●	●	●	●
Minimize exterior signage indicating the presence or locations of assets	WP	WP	WP	WP	WP	WP	WP	WP	WP	WP	●	●

● = Required

WP = Where Practical (if environment is conducive to implement measure)

BP = When Budget Permits

3.3 Specific Criteria (Enhanced Requirements, See Appendix A)

Enhanced requirements will be considered where Design Basis Threat identifies additional risk factors (beyond the baseline).

4 ARCHITECTURE

A great deal can be done architecturally to mitigate security risks to a facility or site. These measures often cost nothing or very little if implemented early in the design process. Architectural considerations include building layout and configuration, space design, and building detailing.

This chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria*. Best Practices are encouraged design considerations, but some or all considerations may be impractical for the project. General Criteria and Space Specific Criteria are OPW requirements which must be met in the project design.

4.1 Principal Best Practices

The design team is encouraged to utilize the following best practices when determining the appropriate and cost-effective measures for incorporation into the building design.

4.1.1 CPTED - Territoriality

a. Interior Design

Although economics and operational issues may sometimes alter this practice, a building's interior spaces may be designed for specific groupings of security layers to discourage wrongdoer activity and keep wrongdoers from vital areas. These factors may cause the occupants to develop a concern for the space immediately adjacent to their office or area. For example, on each floor of a OPW facility, two or three offices areas may share a common corridor area. The office doors would be grouped around that common corridor, and access to elevators or stairs might be screened by a glazed partition not exceeding four feet in height so as to not restrict natural surveillance. The net effect would be the floor's occupants would adopt the corridor as a collective extension of their office (select staff only space) and therefore take an increased interest in the activities taking place there, particularly when accessed by a stranger.

b. Facilities and Amenities

The location of particular facilities (such as employee entrances, employee break areas, and lunch sitting areas) will tend to give an area a high intensity of use and support the idea of territoriality. The presence of staff involved in various activities allows for casual surveillance by concerned staff and screens out possible intruders.

4.1.2 CPTED – Natural Surveillance

A number of concepts have been identified which can be used to design the water and waste water grounds and internal areas around offices, and other areas to facilitate natural monitoring of activities taking place. By providing opportunities for surveillance through the positioning of windows in relation to stairs, corridors, or outside areas, continual natural observation will be maintained and crime will be deterred. If such steps are taken, the security of observed areas will be understood by the potential wrongdoer, making them reluctant to commit a crime at that location.

The first of these natural surveillance concepts involves the positioning of service areas and access paths leading to buildings to facilitate surveillance by staff and security. For example, buildings might be designed so their entries face and are within 15.25 m (50 ft) of a street, so well-lit paths lead to the front door or lobby, and the lobby is arranged to afford good visibility from the street. Other related steps focus on the strategic placement of windows, fire stairwells, lobby lights, trash receptacles, and mailboxes so

they can be easily viewed from the street. Elevator waiting areas on each floor can also be designed so they can be seen from the street level. If steps such as these are taken, building occupants will be more likely to become involved with protecting the facility.

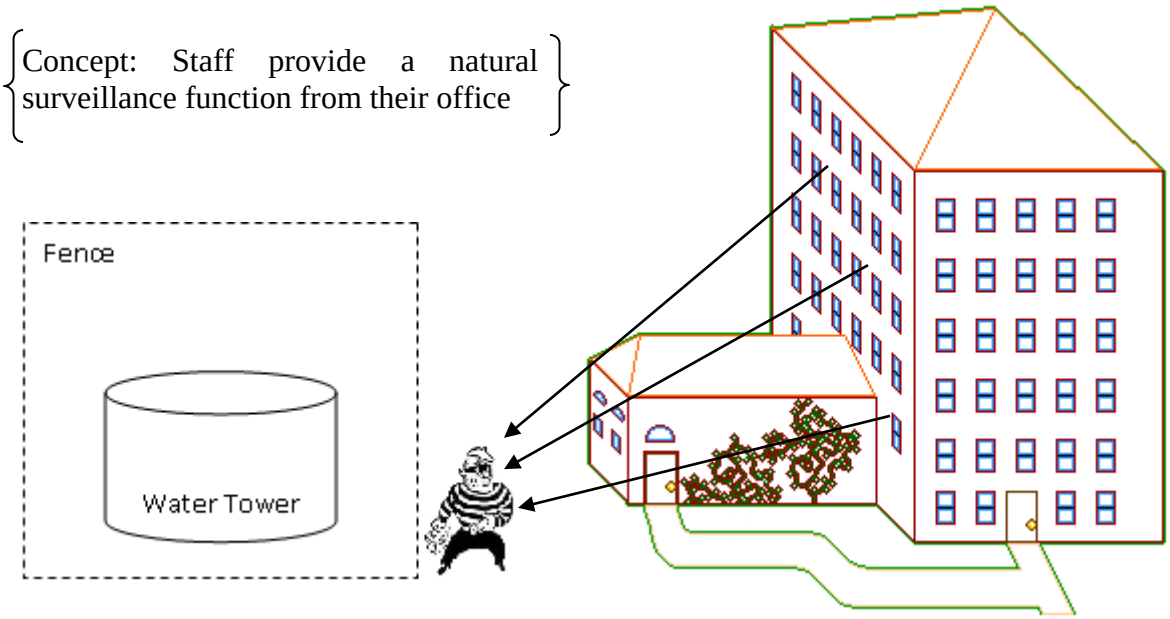


Figure 2 – Natural Surveillance

A second technique (figured above) may be used to increase surveillance is to design facilities so people within them will naturally view commonly used key assets, paths, entries, and play and seating areas during their normal activities. This concept also focuses on the strategic placement of windows, desks, lighting, and open areas so natural surveillance by building occupants is improved.

Another concept involves the subdivision of building areas into small, recognizable, and identifiable groupings which improve visual surveillance possibilities. Research has shown that in office areas where the surveillance of a neighbor's office activities was possible, occupants were found to be very familiar with everyone's comings and goings. The overall effect was to cement collective identity and responsibility through social pressure.

4.1.3 Space Planning & Design

a. The protection of the building interior can be divided into two categories: functional layout and structural layout. In terms of functional layout, public areas such as the lobby, loading dock, mail room, garage, and retail areas need to be separated from the more secured areas of the facility. This can be done by creating internal "hard lines" or buffer zones, using secondary stairwells, elevator shafts, corridors, and storage areas between public and secured areas. The following design measures should be considered:

   1. Locate key assets as far into the interior of a building as possible.
   2. Place areas of high visitor activity away from key assets.
   3. Locate assets in areas where they are visible to more than one person.

4. Eliminate hiding places within the building.
5. Use interior barriers to differentiate levels of security within a building.
6. Stairwells required for emergency egress should be located as remotely as possible from areas where high risk incidents might occur and, wherever possible, should not discharge into lobbies, parking, or loading areas.
7. Consider sheltering in place and assembly areas in space planning.

b. Lobby Areas

In lobby areas the queuing requirements must be incorporated in front of the inspection stations so visitors are not forced to stand outside during inclement weather or in a congested line inside a small lobby while waiting to enter the secured areas.

4.2 General Criteria (Baseline Requirements)

The measures presented here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents. General criteria are baseline requirements that will be implemented. Where measures are deemed impractical due to environmental limitations or funding, consider operational measures that can be implemented. Where baseline measures are not met, a risk measure acceptance should be documented.

	Raw Water		**Wells & Pumping**		**Water Treatment**		**Finished Water Storage**		**Water Distribution**		**Water System Support**	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
Assess and Deploy CPTED principles	●	●	●	●	●	●	●	●	●	●	●	●
Locking cap on aboveground well casing			●	●								
Locking cap on airlines extending through well casing			●	●								
Locking cap on monitoring wells			●	●								
Valve vault hatches – mechanically fastened or locked with shroud over lock			●	●								
Key locked entrance door	●	●	●	●	●	●	●	●	●	●	●	●
Break resistant glass	●	●	●	●	●	●	●	●	●	●	●	●
Windows located away from doors so that intruders cannot unlock the doors through the windows	●	●	●	●	●	●	●	●	●	●	●	●
Locked roof hatches					●	●	●	●			●	●
Roof access ladder with locked shroud	WP	WP			●	●	●	●	●	●	●	●
Chemical fill lines at building exterior – locked access					●	●	●	●			WP	WP
Chemical storage and feed					●	●	●	●			WP	WP

	Raw Water		Wells & Pumping		Water Treatment		Finished Water Storage		Water Distribution		Water System Support	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
equipment locked access												
Clearwell hatch/manway – hardened lock with shroud or mechanically fastened					●	●						
Clearwell vent: gooseneck pipe type – use double screen					●	●						
Clearwell vent: rectangular or circle (larger than pipe)- single layer with shrouded lock					●	●						
Overflow outlet for clearwell: screen and/or flap valve with cage					●	●	●	●				
Access ladder for clearwell - locked shroud					●	●	●	●				
Protective grating or screen to shield open basins from objects that are thrown from outside of the perimeter fence					●	●	●	●				
Tank hatch/manway – mechanically fastened or locked with shroud over lock							●	●				
Tank vent: gooseneck pipe type – double screen							●	●				
Tank vent: rectangular or circle (larger than pipe)- single layer with shrouded lock							●	●				
Locking covers for control, pressure-reducing, air-relief and other valves									●	●		
Locking cover for sampling stations									●	●		

● = Required

WP = Where Practical (if environment is conducive to implement measure)

BP = When Budget Permits

Additional guidance is provided for Baseline Requirements.

a. Entrances

This section provides general requirements for primary and secondary pedestrian entrances, entrance lobbies, employee entrances, loading docks, and other service entrances.

1. Security Guard Post

   All entrances require security monitoring. For water and waste water key offices and water and waste water facilities, guard posts will be located at primary and

secondary building entrances available to the public and staff, this includes loading docks and mailrooms. Guard Posts shall be located where all lobby entrances and pedestrian traffic can be monitored and controlled by security personnel.

If guard stations are located outside, they shall be protected from weather and capable of being secured when not in use.

2. Pedestrian Entrances

   All pedestrian entrances to offices shall be staffed by a security guard force with no automated access control (i.e. card readers).

   a) Public Entrances (Lobby): Based on a Risk Assessment pedestrian screening may be required. Space shall be appropriately sized to match facility size and pedestrian volumes/visitation. See OPW for screening requirements.

   b) Staff Entrances: Staff entrances shall be located independent of main entrance lobbies and be convenient to staff parking. The entrance must be appropriately sized to accommodate guard force operations (Guard Desks, Chairs). Landline communications shall be provided to accommodate guard operations.

3. Screening Devices

   When screening of visitors and packages is required, provide an area with the capacity for screening equipment and queuing area for the anticipated capacity required. At secondary public entrances provide the means to restrict public access to those areas where screening is available when required.

   Where it is necessary to screen people entering a building, permanently install metal detectors and package screening equipment. Where it is necessary to screen people entering a building under specified conditions, provide the required connections for temporary installation of metal detectors and package screening equipment and sufficient space for their installation.

   - Locate screening equipment in a manner which will prevent passage into the building or facility without passing through the devices.
   - When screening devices are not permanently installed, provide secure storage in close proximity to their installation location.
   - Locate screening equipment so as not to restrict emergency egress or reduce the available egress width.
   - Provide sufficient power, telecommunications, and data connections for installation of screening equipment.
   - Provide CCTV camera surveillance and recording of all visitor screening locations.

b. Emergency Generator and Fuel Storage

Emergency and/or stand-by generators and related switchgear may be located in a separate structure from the main building or within the main building.

1. Elevation: The generator room shall not be located at an elevation subject to flooding at any time.
2. Location

a) Prohibited Adjacencies

If within a main building, the generator room shall not be located closer than 15.25 m (50 ft) horizontally or directly above or below:

- Main Entrance Lobby
- Loading Dock
- Mailroom
- Security Operations Center (SOC)

c. Main Utilities

All main utilities such as the main distribution frame (MDF) or electrical switchgear, incoming electrical transformers, etc., will not be located adjacent to public spaces. This requirement does not include utility closets. When feasible, utilities shall be located internal to the building to provide maximum protection from natural and manmade risks. When building codes or operational efficiencies require, main utilities shall be located on exterior walls or the roof of the building where exposure to natural and manmade risks are mitigated. Where feasible, utilities will be collocated in order to consolidate security protection requirements.

d. Public & Staff Separation Portals

Staff only areas shall be grouped to reduce electronic access control requirements. The aggregate groupings of staff spaces shall provide both vertical and horizontal access controls to enable adequate Public / Staff separation. No egress paths from Public space shall pass through Staff only areas.

e. Security Equipment Room (See Appendix C)

At a minimum, the equipment room shall be 18.5 sq m (200 sq ft) and shall scaled up to accommodate electronic security needs of the building or buildings the equipment room will support. Both wall space and floor space requirements shall be considered in sizing the equipment room. Consideration shall be given to building or campus expansion potential. Exceptions to this requirement is for SOCs serving multiple sites, in which case equipment rooms shall be sized to provide additional wall and rack space to accommodate additional equipment. OPW shall be consulted during the space programming phase of the project. The entrance door is to be via the control room; not off a corridor. Surrounding walls and partitions shall be 1-hour fire resistive construction and extend from slab to slab; a 1-hour ceiling assembly may be substituted where slab-to-slab construction is not practical.

1. Wall Space

The equipment room space programming shall consider wall space needs for the following wall mounted equipment. One fourth of the wall space shall be dedicated for emergency power and uninterrupted power source equipment and panels. Another one fourth wall space shall be dedicated to non-Electronic Security Systems, such as fire control and elevator control systems. The remaining wall space shall be dedicated to electronic security systems.

f. Security Control Room

1. Location

The Security Operations Center (SOC) shall not be located below grade for new construction/major modernizations. For existing facilities, Security Operations Center (SOC) will not be located below grade when in a flood zone.

a) Prohibited Adjacencies

This space shall not be located in or adjacent to any public area and not closer than 15.25 m (50 ft) horizontally or directly above or below the following:

- Main Entrance Lobby
- Loading Dock
- Mailroom
- Exterior Wall
- Adjacent to assets

2. Size

A minimum of 37 sq m (400 sq ft) shall be programmed for the Security Operations Center (SOC) console space to accommodate the standard monitoring console and associated monitoring equipment. A minimum ceiling height of 8 ft is required.

Provide wall mounted sound-soak panels to minimize background noise; the panels must meet interior finish requirements for fire safety. A raised computer floor (or depressed slab) is to be provided for this area and the adjacent Equipment Room. Computer floor lift-out panels are to be vinyl tile covered. Refer to Appendix C for standard Security Operations Center (SOC) and console layout and requirements. Changes to the SOC layout shall require OPW written approval.

3. Security Monitoring Console

Refer to Console drawings in Appendix C. The preferred console is a Talon product configured as shown in the console drawings. Changes in console configuration shall require OPW written approval.

4.3 Specific Criteria (Enhanced Requirements, See Appendix A)

Enhanced requirements will be considered where Design Basis Threat identifies additional risk factors (beyond the baseline).

5 STRUCTURAL ENGINEERING

After the site design considerations to enhance protection have been taken into account (recognizing that some may not be applicable to buildings in urban settings), additional building design measures, such as hardening, must be considered to protect building occupants. That is, when the desired level of protection cannot be achieved through site design, building envelope design measures must be considered. Catastrophic collapse of the building is a primary concern. Historically, the majority of fatalities that occur in terrorist attacks directed against buildings are due to building collapse.

The following section provides a precursor and background on structural engineering approach for City of Oxnard, Public Works (OPW) designers. The structural engineering designer should design to the standards available structural design criteria for security. Utilizing the guidance, the structural engineer will determine the building design features needed to achieve the desired level of protection against the design blast threat (if appropriate), considering collapse of the building, as well as injuries and fatalities.

This chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria*. Best Practices are encouraged design considerations, but some or all considerations may be impractical for the project. General Criteria and Space Specific Criteria are OPW requirements which must be met in the project design.

5.1 Principal Best Practices

Design structures to applicable structural codes and standards.

5.2 General Criteria (Baseline Requirements)

The measures presented here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents.

5.2.1 Progressive Collapse

Progressive collapse is a situation where local failure of a primary structural component leads to the collapse of adjoining members, which, in turn, leads to additional collapse. Hence, the total damage is disproportionate to the original cause. Progressive collapse is a chain reaction of structural failures which follows from damage to a relatively small portion of a structure.

All buildings should be designed with the intent of reducing the potential for progressive collapse as a result of an abnormal loading event, regardless of the required level of protection. The following structural characteristics should be considered in the initial phases of structural design. Incorporation of these features will provide a more robust structure and decrease the potential for progressive collapse.

a. Design Considerations

1. Redundancy

   The use of redundant lateral and vertical force resisting systems is highly encouraged when considering progressive collapse. Redundancy tends to promote a more robust structure and helps to ensure alternate load paths are available in the case of a structural element(s) failure. Additionally, redundancy provides multiple locations for yielding to occur, which increases the probability that damage will be constrained.

2. Ductile Structural Elements and Detailing

It is critical that both the primary and secondary structural elements be capable of deforming well beyond the elastic limit, without experiencing structural collapse. The use of ductile construction materials (i.e., steel, cast-in-place reinforced concrete, etc.) for both the structural elements and connection detailing is encouraged. The capability of achieving a ductile response is imperative when considering an extreme redistribution of loading such as that encountered when structural element(s) fail.

3. Capacity for Resisting Load Reversals

   Both the primary and secondary structural elements should be designed to resist load reversals in case of a structural element(s) failure.

4. Capacity for resisting shear failure.

   Primary structural elements maintain sufficient strength and ductility under an abnormal loading event to preclude a shear failure. If the shear capacity is reached before flexural capacity, the sudden, non-ductile failure of the element could potentially lead to a progressive collapse of the structure.

b. Approach

The City of Oxford Public Works takes a threat-independent approach to progressive collapse. The goal of a threat-independent approach is not to prevent collapse from a specific design threat, but to control and stop the continuing spread of damage after localized damage or localized collapse has occurred.

This requires the structural response of a building be analyzed in a test that removes a key structural element (e.g., vertical load carrying column, section of bearing wall, beam) to simulate local damage from an explosion. If effective alternative load paths are available for redistributing the loads, originally supported by the removed structural element, the building has a low potential for progressive collapse. Although these criteria provide specific guidance on which structural elements must be analyzed for removal from the structural design configuration, they do not provide specific guidance for choosing an engineering structural response model for verifying the effectiveness of alternate load paths.

To address blast resistance and to minimize the possibility of progressive collapse, the priority of upgrades should be based on the relative importance of a structural or non-structural element, in the order below:

1. Primary Structural Elements: These are the essential parts of the building's resistance to catastrophic blast loads and progressive collapse (e.g., columns, girders, roof beams, and the main lateral resistance system).
2. Secondary Structural Elements: These include all other load bearing members (e.g., floor beams, slabs).
3. Primary Non-structural Elements: These are the elements (including their attachments) that are essential for life safety systems or elements that can cause substantial injury if failure occurs (e.g., ceilings or heavy suspended mechanical units).
4. Secondary Non-structural Elements: These include elements not covered in primary non-structural elements (e.g., partitions, furniture, and light fixtures).

   Priority should be given to the critical elements which are essential to mitigating the extent of collapse. Designs for secondary structural elements should minimize injury and damage. Consideration should be given to reducing damage

and injury from primary as well as secondary non-structural elements. For example, if an explosive event causes the local failure of one column, which results in major collapse within a structural bay, a design that mitigated progressive collapse would preclude the additional loss of primary structural members beyond this localized damage zone (i.e., the loss of additional columns, main girders, etc.). This would not necessarily preclude the additional loss of secondary structural or non-structural elements outside the initial zone of localized damage, provided the loss of such members is acceptable for that performance level and the loss does not precipitate the onset of progressive collapse.

c. Loads and Stresses

For purposes of designing against progressive collapse, loads should be defined as dead load plus a realistic estimate of actual live load. The value of the live load may be as low as 25 percent of the code-prescribed live load. The design should use ultimate strengths with dynamic enhancements based on strain rates. Allowable responses are generally post elastic.

5.2.2 Existing Facilities

None

5.2.3 New Construction/ Major Modernization

All new construction and major modernizations must be designed to mitigate progressive collapse.

.

5.3 Specific Criteria (Enhanced Requirements See Appendix A)

5.3.1 Existing Facilities

None

5.3.2 New Construction / Major Modernization

All new construction and major modernizations must be designed to mitigate progressive collapse.

6 MECHANICAL ENGINEERING

This chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria*. Best Practices are encouraged design considerations, but some or all considerations may be impractical for the project. General Criteria and Space Specific Criteria are OPW requirements which must be met in the project design

6.1 Principal Best Practices

The design team is encouraged to utilize the following best practices when determining the appropriate and cost-effective measures for incorporation into the building design.

6.1.1 General

Mechanical system design standards address limiting damage to critical infrastructure and protecting building occupants against CBR threats. The primary goal of a mechanical system after a terrorist attack should be to continue to operate key life safety systems. This can be accomplished by locating components in less vulnerable areas, limiting access to mechanical systems, and providing a reasonable amount of redundancy. The Mechanical Engineer shall utilize the following references in their mechanical systems designs; *Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks.*

6.1.2 Design Considerations

During an interior bombing event or fire, smoke removal and control are paramount. The designer should consider the fact that, if window glazing is hardened, a blast may not blow out windows, and smoke may be trapped in the building. The smoke removal system will be essential in the event of a blast, particularly in large open spaces. This equipment should be located away from high-risk areas (e.g., garages and loading docks). The system controls and power wiring to the equipment should be protected and connected to emergency power. Smoke removal equipment should be provided with standalone local control panels which can continue to function independently in the event the control wiring is severed from the main control system. Designers should consider the following:

- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls, but, when this is unavoidable, mount fixtures on a separate wall at least 15.25 cm (6 in) from the exterior wall face.
- Avoid placing plumbing on the roof slab.
- Avoid suspending plumbing fixtures and piping from the ceiling.
- Locate utility systems away from likely areas of potential attack, such as loading docks, lobbies, and parking areas.
- Protect building operational control areas and utility feeds to lessen the negative effects of a blast.
- Design operational redundancies to survive all kinds of attacks.
- Mount all overhead utilities and other fixtures weighing 14 kg (31 lbs) or more to minimize the likelihood they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This

standard does not preclude the need to design equipment mountings for forces required by other criteria such as seismic standards.

6.1.3 Heating, Ventilation, & Air Conditioning (HVAC)

When considering mitigation measures for Chemical, Biological, and Radiological (CBR) hazards, the HVAC systems are of particular concern. A building can provide protection against CBR agents released outdoors if the flow of fresh air is filtered or interrupted.

a. Design Considerations

This section is based on guidance from the Centers for Disease Control (CDC) and National Institute for Occupational Safety & Health (NIOSH). It presents protective measures and actions to safeguard the occupants of a building from CBR threats.

Of particular concern are building HVAC systems, because they can become an entry point and distribution system for airborne hazardous contaminants. Even without special protective systems, buildings can provide protection in varying degrees against airborne hazards that originate outdoors. Conversely, the hazards produced by a release inside a building can be much more severe than a similar release outdoors. Because buildings allow only a limited exchange of air between indoors and outdoors, not only can higher concentrations occur when there is a release inside, but hazards may persist longer indoors.

b. System Considerations

The following design measures from *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks* should be considered to mitigate the risk of CBR threats for buildings as directed by OPW.

- Elevate the fresh-air intakes to reduce the potential for hazardous materials entering a building from a ground-level outdoor release. This has two main benefits. The first benefit is it provides passive security against malicious acts, which makes it more difficult for hazardous material to be inserted directly into the system. The second benefit is that it is less likely that high concentrations of hazardous material will enter the intakes if there is a ground-level release near the building.
- Many existing buildings have air intakes which are located at or below ground level. For those that have wall-mounted or below grade intakes close to the building, the intakes can be elevated by constructing a plenum or external shaft over the intake. An extension height of 3.7 m (12 ft) will place the intake out of reach of individuals without some assistance.
- Cover the intakes by screens so objects cannot be tossed into the intakes or into air wells from the ground. Such screens should be sloped to allow thrown objects to roll or slide off the screen, away from the intake.
- For existing buildings with air intakes below grade, at ground level, or wall-mounted outside secure areas, some protection can be gained with physical security measures (e.g., placing fencing, surveillance cameras, and motion detectors around the intakes to facilitate monitoring by security personnel).
- To prevent widespread dispersion of a contaminant released within lobbies, mailrooms, and loading docks, their HVAC systems should be isolated and the areas maintained at a negative pressure relative to the rest of the building, but at positive pressure relative to the outdoors. A qualified mechanical engineer can assist in determining if the recommended isolation is feasible for a given building.

- Consider shelter-in-place and area of rescue where people can congregate in the event of an outdoor release. The goal is to create areas where outdoor air infiltration is very low. Usually such rooms will be in the inner part of the building in an area with no exterior windows.
- Many central HVAC systems have energy management and control systems that can regulate airflow and pressures within a building on an emergency response basis. Some fire alarm systems provide useful capabilities during CBR events. In some cases, the best response option (given sufficient warning) might be to shut off the building's HVAC and exhaust system(s), thus avoiding the introduction of a CBR agent from outside. In other cases, interior pressure and airflow control may prevent the spread of a CBR agent released in the building and/or ensure the safety of egress pathways. The decision to install emergency control options should be made in consultation with a qualified mechanical engineer who understands the ramifications of various operating modes on building operation and safety systems.
- A rapid response, such as shutting down an HVAC system, may involve closing various dampers, especially those controlling the flow of outdoor air (in the event of an exterior CBR release). When the HVAC system is turned off, the building pressure compared to outdoors may still be negative, drawing outdoor air into the building via many leakage pathways, including the HVAC system. Consideration should be given to installing low leakage dampers to minimize this flow pathway. The speed with which these dampers respond to a "close" instruction can also be important. From a protective standpoint, dampers that respond quickly are preferred over dampers that might take 30 seconds or more to respond.

c. Air Filtration and Pressurization

Among the various protective measures for buildings, high efficiency air filtration/cleaning provides the highest level of protection against an outdoor release of hazardous materials. It can also provide continuous protection, unlike other approaches for which protective measures are initiated upon detecting an airborne hazard.

Two basic methods of applying air filtration to a building are external filtration and internal filtration. External filtration involves drawing air from outside, filtering and/or cleaning it, and discharging the air inside the building or protected zone. This provides the higher level of protection, but involves substantially higher costs. Internal filtration involves drawing air from inside the building, filtering and/or cleaning it, and discharging the air back inside the building.

The relative levels of protection of the two methods can be illustrated in terms of protection factor, and the ratio of external dose and internal dose (concentration integrated over time). External filtration systems with high efficiency filters can yield protection factors greater than 100,000. For internal filtration, the protection factors are likely to be less and are highly variable. The protection of internal filtration varies with a number of factors, including the efficiency of the filter, flow rate of the filter unit, and size of the room or building in which the filter unit operates.

1. Air Filtration and Cleaning Principles

   Air filtration is the removal of particulate contaminants from the air. Air cleaning is the removal of gases or vapors from the air. The collection mechanisms for these two types of systems are very different.

a) Particulate Air Filters

A wide variety of particulate air filters are available to meet many specialized needs. They range from the low efficiency dust filters, such as roll-type filters used in commercial buildings, to HEPA and 'ultra low penetration air' (ULPA) filters used in clean rooms and operating rooms.

HEPA filters are typically rated as 99.97 percent effective in removing dust and particulate matter greater than 0.3 micron in size. Typical HEPA filters have a dip in performance between 0.1 and 0.3 microns; many bacteria and viruses fall into this size range. Fortunately, microbes in this range are also vulnerable to ultraviolet radiation. For this reason, many health care facilities couple particulate air filters with ultraviolet germicidal irradiation (UVGI). UVGI will be discussed later in this section.

b) Sorbent Filters

Particulate filters are not intended to remove gases and vapors. Sorbent filters use one of two mechanisms for capturing and controlling gas-phase air contaminants, physical absorption or chemisorption.

Choosing the appropriate sorbent or sorbents for an airborne contaminant is a complex decision that involves many factors. The installation of sorbent filters for the removal of gaseous contaminants from a building's air is a less common practice than the installation of particulate filtration.

Activated carbon is the most common sorbent. The huge surface area of activated carbon gives it countless bonding sites. Typically, the pores in highly activated carbon have a total surface area of over 1,000 sq. m per gram. Common substances used as a base material for producing carbon are wood, coal, and coconut shell. Impregnating carbon with special chemicals can enhance the absorption of specific gases. A broad-based chemical addition typically used is copper-silver-zinc-molybdenum-triethylenediamine (ASZM-TEDA). Both the Department of State (DOS) and Department of Defense (DoD) currently recommend ASZM-TEDA sorbent for collecting classical chemical warfare agents.

Sorbent filters should be located downstream of the particulate filters. This arrangement allows the sorbent to collect vapors generated from liquid aerosols collected on the particulate filter and reduces the amount of particulate reaching the sorbent. Gas-phase contaminant removal can potentially be a challenging and costly undertaking, and different factors should be addressed.

c) Air Filtration Considerations

In addition to proper filter or sorbent selection, the following must be considered when installing or upgrading filtration systems:

- Filter bypass
- Cost
- Infiltration

d) Ultraviolet Germicidal Irradiation (UVGI)

UVGI has long been used in laboratories and health care facilities. Ultraviolet radiation in the range of 2,250-3,020 Angstroms is lethal to microorganisms.

All viruses and almost all bacteria (excluding spores) are vulnerable to moderate levels of UVGI exposure. Spores, which are larger and more resistant to UVGI than most bacteria, can be effectively removed through high efficiency air filtration. For these reasons, today most UGVI systems are installed in conjunction with high efficiency filtration systems in many health care facilities.

A design utilizing a combination of filtration and UVGI can be very effective against biological agents. Smaller microbes, which are difficult to filter out, tend to be more susceptible to UVGI; while larger microbes, such as spores, which are more resistant to UVGI, tend to be easier to filter out. The design team should consider the addition of UVGI in spaces where there is an increased risk of biological hazard such as the mail room.

In a simulation by the Architectural Engineering Department of Pennsylvania State University, various combinations of MERV and UVGI Rating Values (URV) systems were modeled for a 20-story building subject to releases of anthrax, smallpox, and botulinum. No significant benefits were shown for filtration/URV levels beyond MERV 13/URV 13.2

2. Radiological Hazards Exhausting and Purging

   The primary scenario in which radioactive materials could be dispersed by a terrorist is the use of conventional explosives or other means to spread radioactive materials (a dirty bomb). Filtration and air cleaning devices would be ineffective at stopping the radiation itself; however, they would be useful in collecting the material from which the radiation is emitted. Micrometer-sized aerosols from a radiological event are effectively removed from air streams by HEPA filters. This collection could prevent distribution throughout a building; however, decontamination of the HVAC system would be required.

6.2 General Criteria (Baseline Requirements)

The measures presented here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents. General criteria are baseline requirements that will be implemented. Where measures are deemed impractical due to environmental limitations or funding, consider operational measures that can be implemented. Where baseline measures are not met, a risk measure acceptance should be documented.

	Raw Water		**Wells & Pumping**		**Water Treatment**		**Finished Water Storage**		**Water Distribution**		**Water System Support**	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
Secure mechanical areas with conventional key and lock.	WP	WP			●	●					WP	WP
Monitoring mechanical facilities doors with door position switches	WP	WP			●	●					WP	WP
CCTV camera coverage main access points to main mechanical areas.	WP	WP			●	●					WP	WP
Limit access to air intake vents through use of security fencing	WP	WP			BP	●					WP	WP

	Raw Water		Wells & Pumping		Water Treatment		Finished Water Storage		Water Distribution		Water System Support	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
Access to utility manholes should be within the perimeter	WP	WP			BP	●					WP	WP
Manholes directly outside the perimeter fence should be secured with conventional key and lock	WP	WP			BP	●					WP	WP

● = Required

WP = Where Practical (if environment is conducive to implement measure)

BP = When Budget Permits

Additional guidance is provided for Baseline Requirements.

6.2.1 HVAC

For locations where wall protection is required (see "Walls", paragraph 4.3.2), ducts which penetrate a slab to slab wall and are larger than 240 square cm (37 square in) with any dimension being greater than 15.25 cm (6 in), shall be protected with burglar bars to preclude intrusion. The burglar bars shall be mounted in ducts within fifteen centimeters of the duct penetration through the boundary wall, preferably on the protected side of the boundary wall. Burglar bars shall be #5 rebar (5/8 inch) forming a rectangular web that is welded 125 mm (5 in) on center both horizontally and vertically. Substantial exterior duct support plates and bolts which shall be removable with a special tool are to secure the burglar bars in the ducts. The bars need to be removed when the ducts are in need of cleaning. A duct inspection door is required, on the secure side of the duct grill, to inspect the grill. The installation of burglar bars must not interfere with the installation or ability to inspect/test a fire damper when the two must be collocated.

a. Existing Facilities

None

b. New Construction / Major Modernization

For locations where wall protection is required (see "Walls", paragraph 4.3.2), design ducts penetrating walls to be smaller than 240 square cm (37 square in) with any dimension being greater than 15.25 cm (6 in), if possible.

HVAC requirements should be based on the OPW project specific risk assessment and the following minimum requirements:

1. Maintain positive pressure in lobbies and entrance areas.
2. Locate all fresh air intakes a minimum of 30.5 m (100 ft) from areas where vehicles may be stopped with their engines running.
3. Locate all fresh air intakes a minimum of 12 m (40 ft) above finish grade.

6.2.2 Spaces

a. Loading Dock

Air servicing this area shall not circulate to other parts of the building (dedicated service).

b. Lobby

Air servicing this area shall not circulate to other parts of the building (dedicated service).

c. Mail Room

Air servicing this area shall not circulate to other parts of the building (dedicated service).

d. Security Operations Center (SOC) and Security Equipment Room

Air servicing this area shall not circulate to other parts of the building (dedicated service).

1. A dedicated heating and cooling unit with local thermostat, on emergency power, shall be installed in the Security Equipment Room. The SOC and Security Equipment Room spaces shall be zoned separately or provided with dedicated units to provide dedicated cooling controls. Cooling for the SOC and Security Equipment Room is to meet the heat requirements of the equipment housed. Provide a high temperature device to monitor temperatures that exceed 80 degrees F within the equipment room.
2. Airflow is to enter the front of the equipment racks and be exhausted out the back, with the assistance of fans mounted at the rear of the racks.
3. Provide under floor ducting feeding every other equipment bay (security wiring in open-top Walker-type ducts will use the adjacent bays).

6.3 Specific Criteria (Enhanced Requirements see Appendix A)

6.3.1 Existing Facilities

None

6.3.2 New Construction / Major Modernization

Mechanical requirements are based on the OPW project specific risk assessment.

7 ELECTRICAL ENGINEERING

This chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria*. Best Practices are encouraged design considerations, but some or all considerations may be impractical for the project. General Criteria and Space Specific Criteria are OPW requirements which must be met in the project design.

Use this section in conjunction with the OPW Standard Specification for Electronic Security: 260500 Common Work Results for Electrical, Security Supplement. This specification section contains requirements for conduit and power to support electronic security systems including product specifications, installation standards, and additional submittal requirements.

7.1 Principal Best Practices

The design team is encouraged to utilize the following best practices when determining the appropriate and cost-effective measures for incorporation into the building design.

7.1.1 General

The major security functions of the electrical system are to maintain power to essential building services, particularly those required for life safety and security; provide lighting to aid surveillance which deters criminal activities; and provide emergency communications. Thus, the operability of electrical systems is an important element and is a critical component for life safety systems. Designers should consider the following recommendations:

a. Emergency and normal electric panels, conduits, and switchgear should be installed separately, at different locations, and as far apart as possible. Electric distribution should be run from separate locations.

b. Emergency generators should be located away from loading docks, entrances, and parking. More secure locations include the roof, protected grade level, and protected interior areas.

c. Fuel tanks should be mounted near the generator, given the same protection as the emergency generator, and sized to store an appropriate amount of fuel.

d. A connection should be installed outside to allow a trailer-mounted generator, equal to the building generator, to connect to the building's electrical system. If tertiary power is required, other methods include generators and feeders from alternative substations.

e. Site lighting should be coordinated with the security video system.

f. Emergency lighting should be provided in restrooms.

g. Building access points should be illuminated to aid in natural surveillance.

h. Hardwire emergency lighting in stairwells and exit signs on emergency power circuits. When unachievable, provide self-contained battery lighting in stairwells and for exit signs.

i. Adequate lighting of the perimeter and parking areas should be provided to aid in natural surveillance and support the use of physical security systems.

7.1.2 Lighting

a. General

Lighting should provide for safety and security without compromising the quality of the site, the environment (including neighboring properties), or the architectural character of the buildings. The following are the basic lighting design criteria.

1. Aesthetic: The site lighting should provide desired illumination and enhancement of trees, landscaping, and buildings without providing dark shadowy areas compromising safety and security.
2. Signage: Should be enhanced by site lighting, including providing improved security by assisting pedestrians and vehicles to locate their destinations expeditiously.
3. Environmental: Minimize light pollution and spill into neighboring properties by selection of fixtures' cutoff angles to minimize their nuisance visibility from adjacent areas on and off the property.

7.2 General Criteria (Baseline Requirements)

The measures presented here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents. General criteria are baseline requirements that will be implemented. Where measures are deemed impractical due to environmental limitations or funding, consider operational measures that can be implemented. Where baseline measures are not met, a risk measure acceptance should be documented.

	Raw Water		**Wells & Pumping**		**Water Treatment**		**Finished Water Storage**		**Water Distribution**		**Water System Support**	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
Transformer - locked protective barrier or cage	●	●			●	●	●	●	●	●	●	●
Generator - locked protective barrier or cage	●	●			●	●	●	●	●	●	●	●
Switchgear /motor control center – locked protective cage	●	●			●	●	●	●	●	●	●	●
All electrical panels locked	●	●	●	●	●	●	●	●	●	●	●	●
Backup power to security components (as indicated): UPS, typically	●	●			●	●	●	●	●	●	●	●
All electrical wiring in conduit	●	●	●	●	●	●	●	●	●	●	●	●
SCADA – Locked PLC/RTU enclosures	●	●	●	●	●	●	●	●	●	●	●	●
SCADA - Tamper switch on enclosures	●	●	BP	●	●	●	●	●	BP	●	●	●
SCADA - All instrumentation wiring in conduit	●	●	●	●	●	●	●	●	●	●	●	●
Follow Illuminating Engineering Society of North America (IESNA)for site, asset and building level lighting	●	●	●	●	●	●	●	●	●	●	●	●

● = Required

WP = Where Practical (if environment is conducive to implement measure)

	Raw Water		Wells & Pumping		Water Treatment		Finished Water Storage		Water Distribution		Water System Support	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
BP = When Budget Permits												

Additional guidance is provided for Baseline Requirements.

7.2.1 Large Enclosure Assemblies

A large enclosure assembly may be used in an effort to consolidate space in closets. Large enclosures consolidate security equipment (Data Gathering Panel, Field termination board, such as, I-8 and R-8 boards) and provide for improved wire management. Power supplies shall be located in a separate enclosure.

7.2.2 Security Enclosures and Conduit Systems

The following provides design guidance for the conduit system for ESS.

a. Electrical Metallic Tubing (EMT)

EMT may be used at any point in the system.

b. Closed Tray

Closed tray may be used between the Head-end and Security Closet or DGP. The closed tray shall meet the same marking requirements as security conduit.

c. Common Tray

Security cabling may be run in a common tray with non-security cabling.

d. Exterior Conduits

Utilize schedule 40 PVC pipe. Rigid conduit maybe used in non-corrosive environments.

e. Interior Enclosures

Utilize NEMA 12 rated hinged enclosures. All enclosure will be securable.

f. Exterior Enclosures

Utilize NEMA 4X rated hinged enclosures. All enclosures will be securable.

7.2.3 Lighting

Provide protective lighting in accordance with guidance from the Illuminating Engineering Society of North America (IESNA).

a. Existing Facilities

None

b. New Construction / Major Modernizations

1. Exterior lighting shall be supplemented to assure successful nighttime assessment of perimeter areas using security video systems.
2. Lighting shall be 1-2 foot-candles or greater everywhere within 15.25 m (50 ft) of the building and continuous throughout exterior parking areas and walkways.
3. Security Video: Site lighting shall provide Security Video and other surveillance support with illumination levels and color that assists in proper identification. Lighting shall be coordinated with video cameras to enhance surveillance and

prevent interference. Avoid "blinding" video cameras in the placement and selection of fixtures and their "cutoff" angles. Site lighting shall be uniform with no area having a light to dark ratio of greater than 4:1.

4. Entrance vestibules and loading dock areas shall be illuminated to a minimum of 2 foot-candles within 6 m (20 ft) of the entrance.
5. Night lighting shall be provided in interior spaces to be viewed by security video systems as required. A minimum of 1 foot-candle shall be provided. If 1 foot-candle of illumination is not permitted, coordinate with the security consultant for alternative solutions.
6. Lighting consultants shall consider types of lighting to use that does not hinder or effect closed circuit television. For instance, the use of metal halide is strongly discouraged as it effects CCTVs. Lighting and security consultants shall coordinated location of cameras systems and types of lighting to ensure best of solutions are made.
7. Vehicle Access Control Points: Lighting shall be provided at all vehicle access control points at 3 horizontal foot-candles to assist security officers with visual identification into vehicles and occupants. Where practical, high-mast lighting is recommended, because it gives a broader, more natural light distribution, requires fewer poles (less hazardous to the driver), and is more aesthetically pleasing than standard lighting. Lighting of the entry control point should give drivers a clear view of the gatehouse and, for security personnel, it gives a clear view of the drivers and vehicles.
8. Building entrances and exits: Lighting at building entrances shall support video surveillance and assessment while providing illumination of surfaces and features for safety.
9. Parking areas: All parking areas shall be illuminated in support of video and visual surveillance without objectionable spill into adjacent areas on or off site.
10. Pathways: Pedestrian and bicycle pathways and walks, including bike racks, gates, and other features shall be illuminated in support of video and visual surveillance while providing for safety without objectionable spill onto adjacent areas on and off site.

7.2.4 Power

a. Emergency Power

1. Existing Facilities

   None

2. New Construction / Major Modernizations

   a) Primary power for the security system shall be configured to switch to emergency backup sources automatically if interrupted without degradation of any critical system function. Alarms shall not be generated as a result of power switching, however, an indication of power switching on (on-line source) shall be provided to the alarm monitor.

   b) Emergency Power shall be provided for but not limited to the following:

   - SMS servers, switches, and other rack mounted equipment
   - Activity & Report Printers: Security Operations Center (SOC)

- Video Monitors: Security Operations Center (SOC)
- Intercom Stations
- Radio System
- Lights: Security Operations Center (SOC), Security Equipment Rooms, & Security Offices
- Outlets: Security Outlets dedicated to security equipment racks or security enclosure assemblies. Selected outlets in the security office, supply room, break room and locker rooms
- Security Device Power Supplies (Data Gathering Panel (DGP), Closed Circuit Television (CCTV), Card Access, Lock Power, etc.) powered from the Security Closets or remotely: various locations
- Telephone/Radio Recording Equipment: Security Operations Center (SOC) Security Office
- CCTV Camera Power Supplies: Security Closets
- CCTV Pan/Tilt Units: Various Locations
- Journal/Event/Map Printer: Security Operations Center (SOC)
- CCTV Outdoor Housing Heaters and Blowers: Various Sites
- Intercom Master Control System
- Fiber Optic Receivers/Transmitters
- Security office Weapons Storage
- Outlets that charge handheld radios

b. Uninterruptible Power Supplies (UPS)

In addition to emergency generator power, the following systems must have UPS.

1. Existing Facilities

   None

2. New Construction / Major Modernizations

   a) All UPS for security equipment shall have the capacity to provide one (1) hour of service when emergency generator power is also available or eight (8) hours of service when emergency generator power is not available for normal loads and system activity. All UPS for security equipment must have 20% extra capacity for future expansion. UPS shall be supervised by the alarm annunciation system and report loss of AC power and low battery conditions.

   b) The UPS and panels shall be located within the Security Operations Center (SOC) Equipment Room.

   c) All Security equipment located in Security Closets shall be supported by a minimum of two separate dedicated emergency power circuits and a dedicated UPS.

   d) Dedicated UPS units shall not be floor mounted unless in the SOC. All other UPS units shall be wall mounted with ESS panel assemblies or in an equipment rack.

e) To facilitate spare parts inventory and maintenance contracts, it is requested that the UPS be of the same manufacture as the existing OPW Best Power Technology units.

f) The UPS unit shall provide relay outputs for battery fail, low battery, and AC fail conditions. These relay outputs shall be separately connected to a Security Management System. These alarm inputs shall provide instructions to operations to mitigate the UPS issue.

g) UPS shall be provided for the following:

- SMS servers, switches, and other rack mounted equipment
- Security System Monitors and Keyboards: Security Operations Center (SOC)
- Workstations and additional monitors: SOC Equipment Room
- Communications equipment, system line drivers, and modems for alarm, card access, and CCTV Systems: SOC Equipment Room and various sites.
- CCTV Matrix Switcher: Unit Control Equipment Room
- CCTV: Unit Control Equipment Room
- CCTV Digital Video Recorders, encoders & decoders: SOC Equipment Room
- All SOC Equipment Room rack mounted equipment.

7.2.5 Spaces

a. Security Operations Center (SOC)

1. Power Requirements

a) Provide under-floor outlets on UPS power at the right rear corner of each rack unit. Provide permanent outlet cover power source labels.

b) All low voltage security wiring shall be installed below the raised computer flooring in open-top Walker-type ducts.

c) Miscellaneous Electrical: An independent ground bus shall be provided in the Security Equipment Room, Security Closets and the alarm shop.

d) A duplex outlet is required below each console and equipment bay where emergency power is required. Place outlets below the computer flooring at the left rear console/equipment corner of each bay. Each outlet is to receive a permanent label---no magic marker---identifying the power source as “emergency” and identifying the circuit breaker number; colored receptacles are the preferred method.

2. Security Console Cable Tray

a) Provide an “open top” cable tray under the console and equipment room bays for cable management. Incoming conduit to the rooms should mate with the trough. Elevate the trough above the floor, if the floor is depressed below grade.

b) The electrical trough should enter every other console/equipment bay from one side of the racking, with the HVAC ducting entering the remaining every other bays, and entering from the opposite side of the bays.

3. Lighting
   a) Dimmable lighting shall be provided for general console illumination. Fixture location must be coordinated with the security console layout to provide appropriate lighting at the front edge of the console writing surface.
   b) Fluorescent lighting shall be provided for maintenance work purposes.
   c) Provide a wall mounted battery powered emergency light unit with the light directed at the operator side of the security console.
   d) A sufficient number of fixtures shall be on emergency power to provide 20 foot candles of shadow less illumination in both the Security Operations Center (SOC) and Equipment Room.
4. Telecommunications

   Telephone communications are to be provided at the following locations:
   a) Security Operations Center (SOC): Multiple lines. (Connections placed under the raised computer flooring at the security console.)
   b) SOC Equipment Room: Multiple lines. (Connections placed under the raised computer flooring.)
   c) SOC Equipment Room: A wall mounted jack at 1300 mm (51.2 in) AFF opposite the front side of the equipment racking for a wall phone.

7.3 Specific Criteria (Enhanced Requirements see Appendix A)

7.3.1 Existing Facilities

None

7.3.2 New Construction / Major Modernization

Electrical requirements are based on the OPW project specific risk assessment.

8 FIRE PROTECTION ENGINEERING & LIFE SAFETY

This chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria*. Best Practices are encouraged design considerations, but some or all considerations may be impractical for the project. General Criteria and Space Specific Criteria are OPW requirements which must be met in the project design.

8.1 Principal Best Practices

The design team is encouraged to utilize the following best practices when determining the appropriate and cost-effective measures for incorporation into the building design. The requirements of this chapter must be coordinated with the Fire Marshall with the City of Oxnard Fire Department or AHJ (Authority Having Jurisdiction).

8.1.1 General

The fire protection system inside the building should maintain life safety protection after an incident and allow for safe evacuation of the building when appropriate. Although fire protection systems are designed to perform well during fires, they are not traditionally designed to survive bomb blasts or other disasters. To enhance the performance of fire protection systems, particularly in the case of an explosive blast, the designer should consider the following:

- The fire protection water system should be protected from single-point failure. The incoming line should be encased, buried, or located 15.25 m (50 ft) away from high-risk areas. The interior mains should be looped and sectionalized.
- To increase the reliability of the fire protection system in strategic locations, a dual pump arrangement should be considered, with one electric pump and one diesel pump. The pumps should be located away from each other.

8.2 General Criteria (Baseline Requirements)

The measures presented here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents.

8.2.1 Life Safety

Follow applicable codes.

a. Existing Facilities

None

b. New Construction / Major Modernizations

None

8.2.2 Evacuation

Follow applicable codes.

a. Existing Facilities

None

b. New Construction / Major Modernizations

None

8.2.3 Shelter in Place

Follow applicable codes.

a. Existing Facilities

None

b. New Construction / Major Modernizations

None

8.2.4 Areas of Refuge

Follow applicable codes.

a. Existing Facilities

None

b. New Construction / Major Modernizations

None

8.2.5 Area of Rescue Assistance (ARA) Stations

Refer to applicable codes for requirements.

a. Existing Facilities

None

b. New Construction / Major Modernizations

None

8.2.6 Fire Alarm Monitoring

Where a facility control room is required, a listed computer aided alarm and supervisory signal-processing system will be provided by the project Fire Protection Engineer. The Security Consultant must allocate space in the security console rack for the fire alarm system monitor. The system should be re-settable without the console operator needing to leave his console position.

The facility's fire alarm monitoring panel is to be mounted in the control room; all fire alarm conduit is to be concealed.

a. Existing Facilities

None

b. New Construction / Major Modernizations

None

8.2.7 Fire Alarm Integration with Electronic Security System

All electrically powered door locks at public / staff separations, fire or emergency exit doors, etc. may be designated egress routes. For this reason, the project security and fire protection consultants shall coordinate requirements for fire alarm relays to provide lock release (for those doors within the path of egress) upon fire alarm activation.

As a minimum, each security power supply supporting a locking device shall be equipped with a UL approved relay. Where required electric locks shall be powered through a UL approved relay that releases power to locking devices upon activation of the local fire alarm panel. This shall be coordinated with section 8.2.2 "Evacuation".

The Fire Protection Engineer shall include coordination requirements to provide alarm panel output for the security fire lock relay.

a. Existing Facilities

None

b. New Construction / Major Modernizations

None

8.2.8 Spaces

a. Security Operations Center (SOC)

All conduit and electrical feeds to the fire control panels are to be recessed in the wall. Standard sprinklers shall be provided for the control and computer rooms.

8.3 Specific Criteria (Enhanced Requirements, see Appendix A)

8.3.1 Existing Facilities

None

8.3.2 New Construction / Major Modernization

Security related Fire Protection requirements shall be based on applicable codes, coordinated with AHJ.

9 ELECTRONIC SECURITY

This chapter is broken into three (3) basic sections which are *Best Practices*, *General Criteria*, and *Space Specific Criteria*. Best Practices are encouraged design considerations, but some or all considerations may be impractical for the project. General Criteria and Space Specific Criteria are OPW requirements which must be met in the project design.

Appendixes B and C provide additional information to be used in conjunction with this section in designing the electronic security system. Appendix B provides information and guidance on the type of drawings required by the Security Department (OPW) to document the Electronic Security System. This includes which drawings are required in the various design submission as well as the level of detail expected at each. Appendix C provides standard drawings to demonstrate the level of detail required by OPW.

Use this section in conjunction with the OPW Standard Specification for Electronic Security which includes the following Sections. Contact OPW for copies of the OPW Standard Specification for Electronic Security. If the project only involves security, the Security Designer is responsible for preparing a Division 01 General Requirements specification.

- 260500 – Common Work Results for Electrical – Security Supplement
- 275100 – Distributed Audio-Video Communication Systems – Security Supplement
- 280500 – Common Work Results for Electronic Security
- 280513 – Conductors and Cabling for Electronic Security
- 281300 – Access Control
- 281600 – Intrusion Detection
- 282300 – Video Surveillance

9.1 Principal Best Practices

None

9.2 General Criteria (Baseline Requirements)

The measures presented here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents. General criteria are baseline requirements that will be implemented. Where measures are deemed impractical due to environmental limitations or funding, consider operational measures that can be implemented. Where baseline measures are not met, a risk measure acceptance should be documented.

	Raw Water		**Wells & Pumping**		**Water Treatment**		**Finished Water Storage**		**Water Distribution**		**Water System Support**	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
CCTV – All facility exterior doors					●	●	●	●			●	●
CCTV - Hatches, vaults					●	●	●	●			●	●
CCTV – All facilities vehicle entrances	●	●	BP	BP	●	●	●	●	BP	BP	●	●
CCTV – Site surveillance	●	●	BP	BP	●	●	●	●	BP	BP	●	●
CCTV – Surveillance on Assets	●	●	BP	BP	●	●	●	●	BP	BP	●	●

	Raw Water		Wells & Pumping		Water Treatment		Finished Water Storage		Water Distribution		Water System Support	
	Existing Facility (E) OR New Facility (N)											
Security Measure	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*	*E*	*N*
CCTV – Record all Video Systems at full resolution, 2.5 frames per second and retain video footage for a period of 30 days	●	●	BP	BP	●	●	●	●	BP	BP	●	●
CCTV – Record all alarm activated Video Systems at full resolution, 7.5 frames per second and retain video footage for a period of 45 days	●	●	BP	BP	●	●	●	●	BP	BP	●	●
Security wiring supervised		●		●	●	●	●	●		●	●	●
Electronic Access Controls – On primary facility exterior doors					●	●	●	●			●	●
Electronic Access Controls - on primary site entrance points	●	●			●	●	●	●			●	●
Intrusion Detection – all facility exterior doors					●	●	●	●			●	●
Intrusion Detection – Hatches, vaults					●	●	●	●			●	●
Monitor Electronic Security Activity within a Security Control Room	●	●	BP	BP	●	●	●	●	BP	BP	●	●
Contraband Screening and Detection Building Main Entrances					WP	●					WP	WP
Contraband Screening and Detection on Vehicles entering restricted zones or near assets					WP	●	WP	WP			WP	WP
Staff wear picture identification badges	●	●	●	●	●	●	●	●	●	●	●	●
Visitors wear identification badges	●	●	●	●	●	●	●	●	●	●	●	●
Visitors are escorted in asset areas	●	●	●	●	●	●	●	●	●	●	●	●

● = Required

WP = Where Practical (if environment is conducive to implement measure)

BP = When Budget Permits

Additional guidance is provided for Baseline Requirements.

9.2.1 Security Management System (SMS)

a. System Management Server

Server to be mounted in the equipment room racking.

b. Data Gathering Panel (DGP)

The primary data gathering panel (DGP) shall be Software House ISTAR Pro. System architecture shall be decentralized with DGPs located in Security Closets. Every security device shall communicate with the SMS; the use of local sounders shall not be substituted for the connection to the SMS.

c. Equipment

All ESS subsystems (access control, intrusion detection, video, intercommunications, etc.) shall be furnished with expansion beyond the base project. New construction and major modernizations shall have a minimum of 20% expansion capability. Partial renovations shall have a minimum of 50% expansion based upon the specific project.

All power supplies shall be UL listed.

9.2.2 Access Control

The function of an access control system is to ensure only authorized personnel are permitted into or out of a controlled area. All access control systems control passage by using one or more of the three factors of identification (e.g., something a person knows, something a person has, or something a person is or does). Automated entry control devices based on these factors are grouped into three (3) categories: code, credential, and biometric devices. Keying of access controlled shall be restricted to OPW, OPW shall control all keys for access controlled doors.

All entry control system components requiring interaction with staff or public users shall be mounted in accordance with ADA height requirements, 1,066 mm (42 in) above finished floor (AFF), on the lockset side of the door.

a. Card Readers

Where card readers are required, all doors shall be equipped with conventional key and lock systems regardless of electronic access controls applied. The use of keys to open a door equipped with electronic access controls shall result in a forced open alarm.

The use of electronic access controls is intended for high security areas where an audit trail of access is required, or high throughput locations to reduce the issuance of conventional keys. Electronic access controls shall not be used on personnel offices unless the office is a high security area.

b. Request to Exit Devices

1. Exit shunts mounted in the handles of door hardware is the preferred method. In this situation it is preferred to use a door position switch integrated in the lockset; this cannot be used when a BMS is required.
2. Infrared exit shunts installed at card reader controlled doors will be designed for the following operation:
    a) Infrared exit shunts shall be designed for momentary trigger action.
    b) Infrared exit shunts on doors equipped with electrified locksets shall shunt the door position switch upon exit, but shall not unlock the locking device.
    c) Infrared exit shunts on doors equipped with electromagnetic locks is discouraged; however, when used it shall shunt the door position switch and unlock the locking device upon exit.

c. Door Header Boxes

End-of-line resistors are not to be located within door-header boxes. Provide a Electrical Box, Square, 530 cubic centimeters (1900 Series box Junction boxes) within 3 m (10 ft) above the protected side of the door connected to the door frame with flexible conduit. Locate the resistors in the Junction boxes with use of resistor modules (not hand wired individual resistors). Door Header boxes shall be hinged and secured with approved locking hardware. Tamper monitoring circuit shall be provided.

d. Local Sounders

1. Local sounders shall be installed at all card reader doors.
2. Door prop-open alarms (sounders) should be mounted flush on a stainless steel single-gang box cover, on the protected side, above the door and below any ceiling or tiles. Chime models should be utilized.
3. The local audible sound generating device at all locations shall produce a minimum 92db local chime measured at 3.0 m (10 ft) from the device.
4. Door held-open alarms may be incorporated with request-to-exit devices ONLY if the device will provide the intermittent, chime alert that can be achieved by a stand-alone device.
5. Local sounders shall be programmed to automatically reset upon reset of door position (secured position).

e. Electric Locks

Use of magnetic locking devices is discouraged by OPW. Seek OPW approval when electromagnetic locks must be used in lieu of electric locks (electrical cylindrical locks, mortise locks, or electric strikes). The preferred order of use is as follows:

1. Electrified Cylindrical and Mortise locks
2. Electric Strikes
3. Delayed Egress Locks
4. Electromagnetic Locks (with written OPW approval)
    a) Doors controlled by the access control system shall be controlled by electric strikes which fail secure (unless prohibited by safety code).
    b) Provide power supplies for electric locks with one (1) hour of battery back-up when powered from an emergency power generator circuit or eight (8) hours of battery back-up when not powered from an emergency power source.
    c) Hardware shall comply with NFPA 101.
5. Electrified Cylindrical and Mortise Locks

    Electrified cylindrical and mortise locks are the preferred hardware for electronic access controlled doors.
6. Electric Strikes
    a) The need for door leading edge latch guards should be evaluated where electric strikes are utilized. This is particularly important on doors being retrofitted for electric strikes. All doors with electric strikes shall be provided with free egress hardware, except those equipped with delayed egress hardware.

b) High-current locks (i.e., Von Duprin) require high in-rush current power supplies and NOT the OPW specified power supplies for electrified locksets, electric strikes or conventional magnetic locks. Wire runs must meet manufacturer's requirements.

7. Magnetic Locks

   Magnetic locks are discouraged due to life safety considerations. Where they must be used, only UL listed magnetic lock and egress device configurations with a touch sensitive bar are allowed. Emergency release buttons meeting Americans with Disabilities Act (ADA) distance and height requirements must be provided. Magnetic locks must drop primary power through a relay connection to the fire alarm system. The power drop is not to be controlled by the security management system.

f. Emergency Exits (Delayed Egress Devices)

Any use of Delayed Egress Devices requires Authority Having Jurisdiction (AHJ) approvals

1. A Light Emitting Diode (LED) countdown device should be provided to the right of the door(s) at ADA height. Equipment is to be fail-safe for egress. Video surveillance is to be provided capturing individuals exiting through the door at 'forensic detail'. Delay time for delayed egress hardware is 30 seconds. Nuisance delay time should be set for three seconds. When in fail-safe mode for egress, the hardware should maintain the doors in a fail-secure mode from the outside. Delayed egress devices must drop primary power through a relay connection to the fire alarm system. Only UL listed magnetic lock and egress device configurations with touch sensitive bar or switch in the hardware are allowed.
2. Emergency exit doors must remain latched from the exterior, when the fire alarm system and egress hardware is in emergency exit mode. Emergency exit doors shall not be provided with pull hardware on the exterior side.
3. Delayed egress hardware shall provide status indication through the SMS, not via separate control panels in the security control room.
4. Where delayed egress is required, but local codes may prohibit it, the following shall be substituted: door contact, local sounder, recorded video of individuals and objects being removed, and appropriate signage. Suggested signage is: "Alarm will sound when exiting in non-emergency situations. Under video surveillance."
5. A control shall be required to allow the control room operator to unlock all delayed egress hardware equipped doors simultaneously. See Fire Protection (Section 8) for further guidance.

9.2.3 Intrusion Detection

a. General

Intrusion devices of different technologies (i.e., motion detection, glass break, or magnetic contacts) shall be zoned separately. Intrusion devices of like technologies will be wired together, not to exceed three (3) devices, within the confines of clear physical barriers and not to exceed 15.25 m (50 ft). Devices in the same physical location providing the same purpose shall be programmed in alarm groups to support the Intrusion Zone concept.

1. Sensor Line Supervision

   c) All sensors are to be tampered, reporting trouble regardless of the state of the sensor (on or active, vs. a non-reporting status). Tamper alarms shall be wired to the SMS as a line supervision error alarm zone. Each tamper shall be wired in the sensor circuit to provide a tamper / supervision error.

   a) End-of-line resistors shall be used for the supervision of all alarm devices, and be located at the last device in the circuit, and never at the DGP end of cabling.

   b) End-of-line resistors shall be a prepackaged unit and resistor networks shall meet manufacturers specifications. Resistor quality shall be standard tolerance of 1% or maximum of 1/4 Watt.

2. Mounting Heights

   The mounting heights of all detectors shall be shown on the drawings or in a detail. All motion detectors, glass break sensors and cameras are to be mounted above reach, no less than 2745 mm (9 ft) Above Finished Floor (AFF), if ceiling height permits, to minimize performance degradation through vandalism.

b. Intrusion Zone (Arm/Disarm) Card Readers

Intrusion Zone (Arm/Disarm) Card Readers shall be provided in protected spaces where an intrusion zone is provided. The control device shall shunt the intrusion zone trigger devices upon presentation of proper identification. The control devices shall be applied inside protected areas adjacent to the primary entrance. The control device shall be configured for an adjustable entry /exit delay. Intrusion zones consist of motion detection within the protected area. Perimeter security devices shall not be included on intrusion zones.

c. Intrusion Detection Sensor (IDS) Types

Intrusion Detection Sensors are designed to detect penetration or attempted penetration through perimeter barriers. These barriers include walls, ceilings, duct openings, doors, and windows. IDS are to be placed on any intentional opening. Sensors include but are not limited to the following:

1. Position Switches (Door Position Switches or Balanced Magnetic Switches)

   a) Position switches shall be mounted on the latch edge of the door or opening within 152 mm (6 in) of the latch edge if mounted in the top of the door. Where double doors must be protected, each door shall be fitted with a separate contact sensor. Where doors are controlled by entry control devices, intrusion detection shall be coordinated with authorized accesses to preclude nuisance alarms for authorized entries and exits. Where surface mounted position or balanced magnetic switches are selected, armored cabling shall be routed from the sensor to a junction box location adjacent to or above the opening.

   When using electrified locksets with integrated request-to-exit device, the preferred method is to utilize a door position switch integrated in the lockset; this cannot be used when a BMS is required.

   b) All operable perimeter windows within 4 m (18 ft) of exterior ground surface or within 3 m (12 ft) directly or diagonally opposite a window, structure, fire escape, or roof shall be protected with contact sensors. The sensors shall be individually wired and armed at all times. Exceptions may be granted from

OPW if the windows have burglar bars meeting OPW criteria. An alternative means of protection may be recommended by the security consultant.

c) Card access controlled doors providing access to intrusion zones are to be protected with a Double-Pole, Double-Throw (DPDT) door switch. The first contact circuit shall be wired to the shunt-able input associated with the card reader. The second contact circuit shall be wired into a separate supervised input as the trigger for the intrusion zone. This procedure shall support 'Intrusion Zone' configuration. Ensure this operation coordinates with paragraph "a)" above.

d) Roll-up doors and other doors not a standard size or configuration shall be provided with position switches suitable for the application. Position switches shall be mounted on both the left and right of the protected side of roll-up doors wider than 2 m (6.6 ft).

2. Volumetric Motion Sensors

The number, spacing, and placement of devices shall be in accordance with the manufacturer's specifications to provide 100% coverage of the area to be protected. The area of coverage of each device shall be shown on the drawings.

a) Microwave Motion Sensors

With microwave motion sensors, high-frequency electromagnetic energy is used to detect an intruder's motion within the protected area.

b) Passive Infrared (PIR) Motion Sensors

PIR motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment. The different applications for PIR Motion Sensors include but are not limited to:

- Point - PIR Sensors can be employed so the pattern is focused on a single point such as a door, window, or an fixed object. To include placing a sensor behind an object so if the object is removed the alarm would activate.
- Curtain - A PIR Sensor can be mounted so it creates a field across a path (a "Curtain"). If an intruder passes through this field the alarm would activate.
- 360 - Ceiling mounted PIR Sensors allow a full 360 degree range of sight. Therefore, if an intruder entered an area from an opening the alarm would activate.

c) Dual Technology Sensors

To minimize the generation of alarms caused by sources other than intruders, dual- technology sensors combine two different technologies in one unit. Ideally, this is achieved by combining two sensors that individually have a high probability of detection (POD) and do not respond to common sources of false alarms. Available dual technology sensors combine an active ultrasonic or microwave sensor with a PIR sensor. The alarms from each sensor are logically combined in an "and" configuration (i.e., nearly simultaneous alarms from both active and passive sensors are needed to produce a valid alarm).

3. Glass-Breakage Sensors

   The number, spacing, and placement of devices shall be in accordance with the manufacturer's specifications to provide 100% coverage of the boundary to be protected. The area of coverage of each device shall be shown on the drawings.

   a) Acoustic glass break sensors or shock sensors shall be provided for the protection of glass panels that exceed 240 square cm (37.2 square in) with any dimension greater than 200 mm (8 in).

   b) Seismic sensors shall be provided for situations where acoustic glass break sensor performance is degraded such as blast windows, laminated glass, or glass with security or fragment retention film.

4. Duct Sensors/Detectors

   A duct is considered an intentional opening and part of the boundary layer. Sensors shall be mounted on the secure side of an opening to detect intrusion. Detection may be provided by one or a combination of motion detection, contacts or barrier bars, tension wires, or pressure mats within the duct. The designer may submit alternative detection methods to OPW for approval. The designer is responsible for selecting the appropriate sensor technology based upon the project conditions. The existence of a physical barrier (burglar bars or grates) does not eliminate the need for intrusion detection device.

   For locations where wall protection is required (see "Walls", paragraph 4.3.2), design ducts penetrating walls to be smaller than 240 square cm (37 square in) with any dimension being greater than 15.25 cm (6 in), if possible. Another option is to design frequent angles to make passage difficult. Seek guidance from OPW. If penetrations cannot be designed to prevent intrusion then apply duct detection.

   a) Motion Detection

      Motion detection is the preferred method to detect intrusion through ducts. However, when two layers of protection are required, another form (of a differing technology) is required.

   b) Pressure Sensitive Barrier Bars

      Pressure sensitive barrier bars are an acceptable means of detecting passage through a duct or protected opening. Barrier bars may also be used within a duct at the perimeter of a space to reduce the opening to smaller than man-passable (a clear cross section area of 619 square cm (96 square in) or more with the smallest dimension exceeding 15.2 cm (6 in)). Add the optional vertical cross bars as necessary to reduce the size of the opening.

      Barrier Bars shall be constructed of metal and use mercury switches to detect attempted removal. Barrier bars shall be securely fastened to the surrounding building material in a manner such that the attempted removal of the vent cover or the barrier bar causes the sensor to activate. Mount barrier bars on the secure side of the opening to minimize tampering. Barrier bars shall not restrict air flow through the vent.

   c) Tension Wires

      Tension wires detect changes in the tension on a wire caused by cutting of the wire or increased pressure on the wire. Tension wires could be used to dissect the opening into smaller openings

d) Pressure Mat

A pressure mat may be located within the duct to detect the weight of an intruder within the duct.

d. Intrusion Detection Sensors (IDS) Applications

The following are examples of typical application of IDS on intentional openings:

1. Doors: Typically protected with door position switches with PIR motion sensors as a back-up system if necessary.
2. Windows / Glazed Openings: Typically protected with position switches and glass break sensors with PIR motion sensors as a back-up system if necessary.
3. Archways: Typically protected with a PIR curtain motion sensor.
4. Vents / Ducts: whenever possible, vents / ducts should be designed to be smaller than man-passable (a clear cross section area of 619 square cm (96 square in) or more with the smallest dimension exceeding 15.2 cm (6 in)). When this is not possible, they should be protected in a manner described above.

e. Video Analytics

Video analytics may be used in lieu of other identified detection technologies. OPW shall be consulted prior to planning to use video analytics. Video analytics will be a integrated element of the overall security management system. Third party platforms are not to be used, unless special features sets are required to mitigate threat. This platform will be signed off by the director level.

f. General Wireless Alarm Systems

The Wireless alarm system shall be a spread spectrum, 900 MHz system with field repeaters as necessary. It should be provided with sufficient zoning to handle anticipated use and a minimum of 16-channel wireless panels are the system of choice, mounted in Security Closets at 1500 mm (59 in) AFF. Repeaters may be required to achieve a minimal signal test level of “10” with the test kit.

1. Receivers
   a) Receivers must have a relay output to the SMS for each zone, and the preferred unit should accommodate 16 zones (at a minimum) with 64 transmitters. A 17th zone must report supervisory errors.
   b) All receivers, whether single or multiple zone, shall be field programmable (as opposed to factory setting).
   c) Receivers must be contained within alarmed Security Closets and mounted on steel enclosures. Receivers shall be mounted on the front covers of locked steel enclosures, to permit conduit to be run from the steel enclosure. Wiring is to be routed in a protected manner, out the rear of the receiver into the steel enclosure.
   d) Each receiver is to be given its own house code, from a master list maintained by OPW. The house code is to be permanently displayed on the metal cover of the steel mounting enclosure.
2. Repeaters
   a) The placement of repeaters is critical. Signal strength tests are required to determine their need and placement.

b) In determining the need (or non-need) for a repeater, the consultant during design---and the installation contractor during installation---must conduct field strength tests with the appropriate test kit. (Testing during construction is imperative because local field conditions may have change with the introduction of steel.) A radio frequency signal indicator reading below 10 between the transmitter in the field and the receiver is unacceptable. Both the consultant and the installer are responsible for providing the test kit.

c) Repeaters mounted in accessible locations must be wired with an external tamper alarm switch inside the plastic cover, and wired to the "external terminal". Repeaters shall be powered from the DGP power supply at the nearest Security Closet. Under this situation, battery back-up is not needed in the repeater housing. Repeaters shall not be mounted lower than 2745 mm (9 ft) AFF.

g. Weapons Containers and Safes, if available

Weapons containers shall be protected in accordance with UL Safe "Partial Protection" with door contacts only. These sensors shall be annunciated through the alarm annunciation system.

Safes shall be provided with door opening contacts and vibration detection in accordance with UL Safe "Complete Protection".

h. ATM Machines, if available

All ATM machines should be outfitted with a common alarm output for connection to the SMS.

9.2.4 Video Surveillance & Assessment

a. Resolution

The following resolution levels shall be utilized in conjunction with the space specific criteria found in the measures.

1. General Surveillance Detail

   This video shall provide a minimum of 20 pixels per foot. This level of detail is often desired for live viewing where the detail is not necessary on recorded video. For instance, looking to see what a crowd is doing without needing to recognize faces. Or only needing to detect when someone is in a restricted area.

2. Forensic Detail

   This video shall provide a minimum of 40 pixels per foot. This level of detail is necessary when it is desired to see, record, and recognize images like license plates and faces. This allows the video to be referenced after an incident to determine exactly what happened and provide forensic evidence.

3. High Detail

   This video shall provide a minimum of 80 pixels per foot. This level of detail is applicable in a retail or banking context where there is a need to clearly see the customer's and employee's faces as well as identify the currency in their hands.

b. Assessment Video

Assessment cameras shall be alarm actuated by either intrusion detection sensors or entry control devices. Views shall be installed and configured so that alarms are presented at the security console, the appropriate image is also displayed at the console within 1 second.

c. Video Recording and Storage

At a minimum, all camera video shall be recorded at 2.5 images-per-second for 24 hours a day, seven days a week and stored for thirty (30) days. Alarm or event actuated video shall be recorded at fifteen (15) images-per-second starting fifteen seconds before the alarm event occurs and lasting one minute after the alarm is cleared.

d. Cameras

Fixed cameras shall be specified for applications requiring continuous video capture. Pan-tilt-zoom (PTZ) cameras may be utilized for general surveillance and/or alarm actuated events in conjunction with preset positions.

1. All cameras shall be color day/night. All interior cameras shall have dome enclosures. All exterior cameras will be housed in environmentally controlled domes unless operational requirements make a dome unnecessary; in that instance, an environmentally controlled enclosure may be utilized.
2. Provide alternative illumination such as IR or thermal for spaces or areas requiring low light.
3. The mounting heights of all cameras shall be shown on the drawings or in a detail. All cameras are to be mounted above reach, no less than 2745 mm (9 ft) AFF if ceiling height permits. This minimizes performance degradation through vandalism.
4. A field of view is to be shown by dashed lines (or shading) on drawings indicating the intended view of each camera.

e. Video Storage

Matrix storage systems will be network based digital video systems with integration to the Software House Video Management System and enterprise level. The system will be utilize be all City of Oxford, Public Works facilities. Monitoring or viewing stations will be based on the use of the native software offered by the video management system.

9.2.5 Spaces

a. Site

Site surveillance of exterior walls, adjacent grounds up to 9 m (30 ft) from the building, and of pedestrian paths. 100% video coverage is required, through the use of Pan-Tilt-Zoom dome cameras which are available for alarm call-up. Vehicle entry points shall be provided with fixed cameras with forensic quality video of vehicles entering and exiting.

b. Loading Docks, and Parking Areas

1. Video Surveillance & Assessment

   Provide video surveillance of all loading dock areas, including the roll down gate, vehicle inspection areas, parked vehicles, loading and unloading activities, and building entrances at the loading dock to supplement the view of the loading dock officer. The images shall be recorded in the SOC with all other security video. Remote monitoring station shall be provided for loading dock and parking staff.

2. Parking Areas

   Provide general video surveillance of public and staff parking areas.

c. Assets

Video surveillance of all assets will be provided based on risk value.

d. Security Operations Center (SOC)

The Security Operations Center (SOC) and operator workstations shall be designed in accordance with the OPW standard design as provided in Appendix C of this document. The SOC is intended for monitoring purposes only, all head-end equipment shall be located in the associated Equipment Room.

e. Security Equipment Room

The Equipment Room shall be designed in accordance with the OPW standard design as provided in Appendix C of this document.

1. Rack Space

   Sufficient space shall be provided to accommodate 100% system growth. Refer to standard specifications for rack system requirements. Computer racking shall be centered in the room, permitting access doors to be opened on all sides. Maintain minimum required electrical code distances from the UPS.

2. A 19 mm (0.75 in) fire-rated plywood (or comparable material) shall cover the three walls of the Security Closet, not including the wall with the entrance door if equipment is not to be mounted there.
3. All incoming and outgoing conduit shall terminate/originate at metal wire troughs mounted above the security equipment cabinets.
4. All alarm equipment, DGP, hubs, converters, and electric locks are to be provided with eight (8) hours of battery backup and on emergency generator circuit to provide uninterrupted service.

9.3 Specific Criteria (Enhanced Requirements, see Appendix A)

Refer to Appendix A to identify space classifications and specific security measures required.

Appendices

A. APPENDIX A – ENHANCED SECURITY MEASURES

1. This section benchmarks general design basis of threat across water and waste water facilities. It establishes the objectives and motivations of four aggressors (vandals, criminals, saboteurs and insiders). While this table provides a generalized understanding of the threat basis, it does not attempt to identify all threats particular those associated with a given facility. There are factors beyond the scope of the enhanced measures that require a further understanding of threats associated with a given facility. The table does provide general factors that are considered a benchmarked understanding of aggressors.

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

2. The section coincides with the master plan document and when performing the risk assessment (threats, vulnerabilities, etc.) should be utilized in conjunction the *Guidelines for the Physical Security of Wastewater / Stormwater Utilities, ANSI/ASCE/EWRI 57-10 as a whole including the use of countermeasure sections as it relates to each the facility type.*

3. The facility owner, project team which should include a security consultant; will utilize this section as a supportive decision making tool to outline specific measures to create an enhance level of security.

A. APPENDIX B – STANDARD DESIGN SUBMISSIONS

1. General Information

   This appendix contains information and guidance on the type of drawings and other deliverables required to adequately detail and document the Electronic Security System design. Also included is guidance about the drawings and other deliverables required for the various design submissions throughout the typical design process.

2. General Drawings

   a. Coversheet

      The cover sheet bears general project information. The consultant is responsible for obtaining specific cover sheet lay out information from SI. The cover will shall, at a minimum, bear the following information:

      i. Project Name
      ii. Project Address
      iii. Project Code
      iv. Submission Date
      v. Design Team/Firm Information
      vi. Project Rendering/Illustration
      vii. Project Site Map
      viii. Project Area Map
      ix. Title Block (Title block shall be on each sheet of the procurement package)
         - Sheet Number
         - Project Name
         - Revision Number
         - Design Firm Name
         - Professional Engineer's Seal (Upon Request)

   b. Index Sheet

      The index sheet shall be used as a general reference for the procurement package. The index sheet shall convey limited project information in the form of "General Notes"; for more comprehensive understanding of the project and design intent the Consultant/Contractor shall reference the appropriate project specification. The Consultant/Contractor shall use the index sheet to display the various symbols and abbreviations used within the drawing set. The index sheet shall also bear a complete listing of the procurement package's contents, to include the numbers and material contained on each sheet.

   c. Site Drawing

      The site drawing shall depict the in scope area surrounding the project building. The Consultant/Contractor shall use site drawings to show utility routes, topology, and site level equipment.

   d. Floor Plans

Floor plans shall depict specific project areas. The drawings shall be to scale and will include rooms w/room names, partitions, elevators, equipment, conduit etc. The floor plans will be a depiction of current or future conditions.

e. Riser Diagrams

Riser diagrams shall depict the vertical and lateral routing of conduit systems. A cross section of the specific building is typically used to show the approximate location of the conduit. Symbols for the project specific security equipment may be used to provide reference points. Each subsystem requires a separate riser diagram.

f. System Interconnect Drawings

System interconnect drawings shall be used as an aide in connecting and terminating system equipment. Detailed representations of security equipment enclosures and circuit card assemblies shall be show. Graphical representations of the prescribed wire types shall be used to depict the point-to-point connections.

g. One-Line Diagrams (Block Diagrams)

One-line or block diagrams shall be used to provided a general overview of the interconnections of the electronic security system components. Each subsystem requires a separate one-line diagram.

h. Equipment Schedule

Equipment Schedules are detailed lists of the electronic security system's components. The equipment schedule will include the following at a minimum:

i. Component Name
ii. Manufacturer
iii. Part Number
iv. Quantity

i. Wire Schedule

Wire schedules are detailed lists of the wires and cables used to connect and terminate the electronic components security system. The wire schedule will include the following at a minimum:

i. Wire Type
ii. Manufacturer
iii. Part Number
iv. Quantity
v. Related Electronic Security System Component (a separate table may be used)

j. Door Schedule

Door schedules are detailed lists of all doors that have special security requirements. The door schedule shall include door type (corresponding with door details), door number, room description, sheet referred, types of hardware used (door contact with description, card reader with description, duress, sounder, locks types, intercom with description, camera reference), and

hardware mounting type (recessed or surface). Any space that requires a access control or intrusion detection measure, shall be listed in the door schedule with each special security measure identified.

3. Standard Details

   Standard details are used to show detailed representations of the electronic security system's components and the variations of component configurations.

   a. Door Details

      Door details (or door elevations) shall depict the typical configuration of access control system (ACS) equipment, intrusion detection system (IDS) devices, and door hardware associated with a particular door. A separate door detail will be provided for each variation or special condition. The detail(s) shall include notes that outline typical mounting instructions, basic connection and termination instructions, supervision requirements, and other pertinent information not conveyed by the detail alone.

      Door Details shall include, but are not limited to the following:

      i. Double Door Elevation
         - ACS Variations
         - IDS Variation
         - Fire Door Package

      ii. Single Door Elevation
         - ACS Variation
         - IDS Variation
         - Fire Door Package

      iii. Overhead Door Elevation:

      iv. Roof Hatch Elevation

   b. Closet Assembly Details

      Closet assembly details shall depict the electronic security system components relative to the electrical or telecoms closet they are mounted in. The detail(s) shall include notes that outline typical mounting instructions, basic connection and termination instructions, supervision requirements, and other pertinent information not conveyed by the detail alone. A closet assembly detail shall include, but is not limited to the following:

      i. Field Panels

      ii. Field Panel and Lock Power Supplies

      iii. Camera Power Supplies

      iv. Network Switches

      v. Fiber Optic Hubs

      vi. Input Board Enclosures

      vii. Relay Enclosures

      viii. Cable Trays/Wire Ways

ix. Interconnecting Conduit

c. Equipment Details

Equipment details shall depict detailed graphical representations of the electronic security system components. The detail(s) shall include notes that outline typical mounting instructions, basic connection and termination instructions, supervision requirements, and other pertinent information not conveyed by the detail alone.

A detail shall be provided for each major component to include, but not limited to:

i. Camera
ii. Network Video Recorder
iii. Access Control Field Panel
iv. Card Reader
v. Reader Module
vi. Request-to-Exit Device
vii. Door Contact

d. Security Console Details

Security console details shall provide a detailed graphical representation of the security console. The detail(s) shall depict console configuration with measurements. The detail shall include notes on the configuration of the console and other pertinent information not conveyed by the detail alone.

Security Console Detail shall include, but is not limited to:

i. Command Center Layout
ii. Security Console
iii. Workstation
iv. Free Standing Racks
v. Rack Mounted Equipment

4. Project Deliverables

a. Basis of Design

Prepare a section of the Basis of Design Narrative describing the physical and electronic security systems measures proposed for the project. Incorporate the security requirements provided in the body of this document and Appendix A and identifying exceptions to those requirements. In addition, make recommendations for deviations from the requirements.

b. Schematic Design

Prepare a section of the Schematic Design Narrative describing the physical and electronic security systems measures proposed for the project. Incorporate the security requirements provided in the body of this document and Appendix A and identifying exceptions to those requirements. In addition, make recommendations for deviations from the requirements.

c. 35% design documents

At 35% OPW the deliverable shall include the following:

i. Coversheet with Project Title, Site and Vicinity Plan.
ii. Information Sheet containing general notes, abbreviations, symbols and conventions, index of sheets, and wire and cable schedule.
iii. Floor plans with area classifications and proposed ESS device placements
iv. Preliminary riser and one-line diagrams for ESS
v. Provide product datasheets of all ESS equipment including the data transmission system
vi. Outline specifications
vii. Project narrative and description to be included with Outline specification above.

d. 65% design development Documents

At 65% DD submission, the design shall include the following:

i. Includes all documents identified in 35% submission documents
ii. Floor plans improved with reflected ceiling plans, system point numbering, and sized conduit routing shown.
iii. Power/UPS Sources Requirements
iv. Sensor Installation Details/Wiring Block Diagrams
v. Mounting details for all ESS devices /Wiring Block Diagrams
vi. Door Details /Wiring Block Diagrams
vii. Riser and One-line diagrams with system points and required cabling types and counts
viii. Door Schedule
ix. Project Specifications– based on a customized version of the Construction Specifications for Electronic Security.
x. System Point Loading Sheets (Istar)

e. 95% Construction Documents

At 95% CD submission, the design shall include the following:

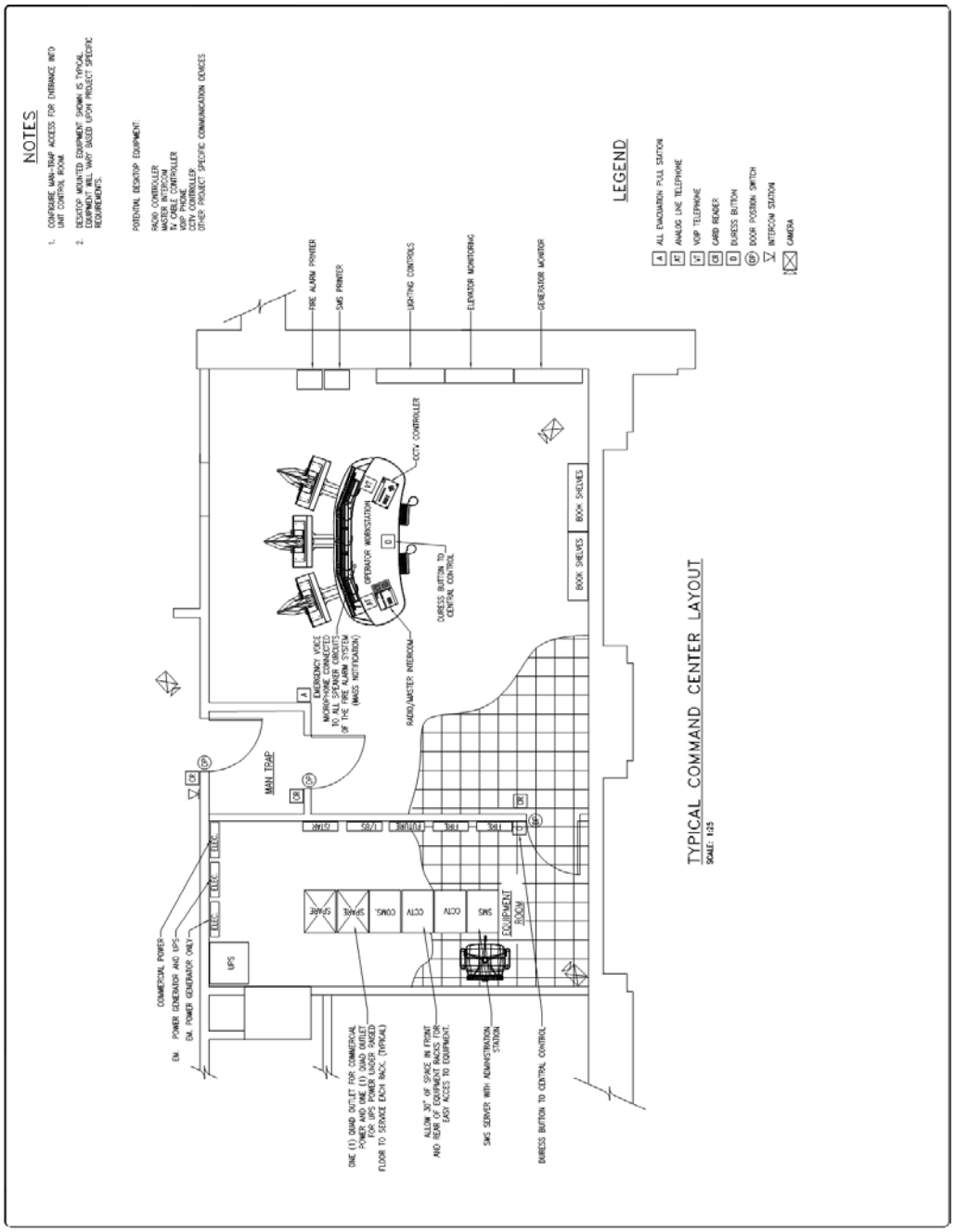
i. Includes all document identified in 35% and 65% submission documents
ii. Elevator Control Interface Plan Development
iii. Cutover Implementation Schedule
iv. Manufacturers Hardware and Software Data
v. System Description and Analysis
vi. 100% final Construction Documents

Includes all previous submission content. This submission shall only be minor corrections and changes by OPW.

B. APPENDIX C – STANDARD DRAWINGS

The drawings listing are standard drawings typically include in conventional electronic security designs.

1. Security Console Details
    a. SOC Console
    b. SOC Room & Equipment Room



C. **APPENDIX D – STANDARD SPECIFICATION OUTLINE**

1. Security Systems

   All security systems by design will reside on a newly established dedicated digital security system network that will provide a secure site wide communication platform that is isolated from the operations network for the City of Oxnard Public Works. The electronic security measures, combined with the physical security control hardware, will permit the OPW organization security operations center the ability to monitor and control all security system elements for the Public Works department. The electronic security design section will include the following classification of security systems.

2. *Physical Access Control System (PACS) – Division 28 13 00*

   a. The system design will provide a new digital physical access control system for integration to the OPW dedicated Security Operations Center (SOC). The physical access control system will provide the visual feedback of status and for operational control of specific field devices and display visual alarm conditions at the SOC console when events are generated by the physical access control system, alarm sensors, or devices controlled / monitored.

   b. The physical access control system will provide the primary operational control of all credential access points, perimeter entry points, and associated alarm sensors. The access system will provide the automated control of authorized valid entries at any portal (i.e. vehicle, pedestrian) access point electronically controlled electrified lock hardware, and motorized gates, motorized vehicle barriers, parking barriers, and door position sensors. The PACS will be equipped for intrusion detection (UL1076 compliant) providing intrusion type alarm monitoring features. Access into physical access controlled areas will require the utilization of an authorized credential (dual frequency 13.56 MHz and Legacy 125 KHz) compatible readers. All perimeter doors along with doors separating public from staff areas will be equipped with card readers with pin. The physical access control system will be ready for integration with the video surveillance system software applications to provide event driven incident recording and logging of associated cameras.

   c. The primary SOC will have full access and control of all networked security physical access control related system functions via the site wide security system network solution. This SOC console will have remote control, display, and monitor all security related systems through a dedicated amalgamated security management system solution. These authorized security control center operators will have full access and control of the distributed access control system controllers and alarm monitoring features via the physical access control system software. The authorized operators will be able to monitor and control the physical access control system for access, denied access, tracing, PIN validation, request-to-exit (REX), door position, forced door, propped door status at all times.

   d. Personnel duress system consisting of fixed panic buttons will be provided at locations of risk including public interaction locations. The fixed panic button system will consist of both wall mounted and "under the desk" panic switches,

where indicated on the drawings. Activation of any panic pushbutton will sound an audible tone in the control room and cause the associated graphic panel duress LED to flash along with activation of nearest cameras to provide the SOC console operator with a visual assessment of the alarm condition. The audible tone may be silenced at which time, the icon will illuminate steady. The control panel may not be cleared until the panic device has been reset. The system will interface with the overall computer based security system as specified. Alarms will annunciate on the control terminal console as specified and be electronically integrated to activate any associated CCTV cameras or other electronic monitoring systems within the alarm zone as may be required.

e. Intrusion detection devices will be provided on critical infrastructure systems (generator, HVAC, etc.).

f. The PACS will be the Software House CCURE 9000 system.

3. Video Assessment Surveillance System (VASS) – Division 28 23 00

a. The contractor will provide a new Video Assessment Surveillance System (VASS) located within the SOC. The VASS will provide local operational control and alarm assessment recording of all cameras. The VASS's primary function is to maintain a video record of events and provide real-time assessment opportunities of incidents at the site location. The VASS will have the ability to be monitored and controlled from SOC Console along with any client desired workstation. All client workstations will have full access and control of all VASS functions via remote connections on the local area network (LAN) and using VASS software. The workstation operators will have the ability to activate per camera call-ups to pre-positioned presets, mask offsite camera views, and perform camera patrols as determined OPW authorized users and will be able to control with network client software connected to the local area dark network (LAN), the network video recorder and associated cameras via integrated software.

b. IP based 1080P (2.1 MPx 1920 x 1080; 16:9 aspect ratio) cameras will be placed at all facility entry points, Public Lobby and asset locations to monitor egress along with entry into any secured internal corridors and departments including loading dock, water resources, utility areas, and security and IT rooms. Exterior cameras will also be utilized to provide complete visual surveillance of the facility perimeter and parking areas. All cameras will be vandal resistant and low light capable.

c. The local network video recorder storage system will be so designed to record and retain video images from each camera at no less than 15 images-per-second and at full native digital resolution of the cameras for a period of no less than 30 days.

d. All recording and retention for all facilities will reside in the OPW SOC Equipment Room. Local recording may be at the local facility via on board camera recording or local recording systems.

e. The VASS will be Milestone Xprotect Corporate Edition.

APPENDIX C – PHYSICAL SECURITY NEEDS ASSESSMENT – MAINTENANCE SERVICE CENTER

PHYSICAL SECURITY NEEDS ASSESSMENT

Prepared For

CITY OF OXNARD CALIFORNIA

MAINTENANCE SERVICE CENTER

1060 Pacific Avenue
Oxnard, California 93030

Prepared by

Summers Associates, LLC
Consulting & Design
"Making our world a safer place by design"

On Behalf of

carollo
Engineers...Working Wonders With Water®

June 2016

Table of Contents

PHYSICAL SECURITY NEEDS ASSESSMENT

PART I OVERVIEW

1.1 Background

Carollo Engineers, Inc. (Carollo) contracted Summers Associates, LLC, an independent security consulting firm, to perform a *Physical Security Needs Assessment* of the *Maintenance Service Center* (MSC) located at 1060 Pacific Avenue, Oxnard CA 93030. This assessment follows on the heels of a Security Master Plan report assessing assets under the auspices of the City of Oxnard Public Works Division, Utility Service Branch.

The Maintenance Service Center (MSC) serves as base for the following City operations:

- Fleet Services Division
- Parks Division
- Facilities Division
- Capital Projects Management
- Graffiti Action Program

Additional property descriptors include:

- Lot size: ±10 acres.
- Property Perimeter Length: ±2,600 ft.
- Location: Southeast corner of Pacific Avenue and Wooley Road.
- Perimeter Vehicle Entrances: 3.
- Perimeter Pedestrian Entrances: 1.
- Adjacent Businesses:
    - Dandy Cooling
    - Duda Farm Fresh Foods
    - Western Pre-Cooling
    - Silvas Oil
    - Southern California Gas
    - Gills Onions

1.2 Methodology

A Physical Security Needs Assessment provides decision-makers with an evaluation of physical security systems and countermeasures in their current state. Security strengths and weakness have been identified with recommendations for improving conditions have

been through corrective measures. As used in this report, the term “physical security” is defined as that part of a security program concerned with physical measures designed to safeguard personnel and property from attack by a malevolent human adversary.

As requested, Summers Associates performed the following tasks associated within the Physical Security Needs Assessment:

Task A: Conduct a physical security needs assessment of the City Corporate Yard facility.

Task B: Evaluate all existing physical and electronic security countermeasures.

Task C: Evaluate facility site perimeter.

Task D: Review incident history.

Task E: Provide a draft written report with findings and prioritized recommendations with associated costs where applicable. Summers Associates will then finalize the report and present one (1) electronic copy of the report.

The following individual offered their time, input and insights which aided in the completion of this plan:

- Art Gutierrez, Facilities Maintenance Supervisor

1.3 Scope of Report

The scope of this report is limited to the evaluation of physical security systems and assets at 1600 Pacific Avenue, a 10-acre parcel located in a light industrial district southeast of downtown Oxnard (Figure 1). This report is not a comprehensive risk analysis or vulnerability assessment, nor does it consider all hazards[1]; it focuses strategies on safeguarding the facility from attack by malevolent human adversaries.

1.4 Targets and Attackers

The motivations for an attack on a public facility are varied but are well classified in the following four categories:

- **Vandal** – Damages or destroys assets for thrill, dare, or grudge.
- **Criminal** – Theft of valuable assets for financial gain or grudge.

[1] “All Hazards” is well defined by ANSI/AWWA G430-14 (2014) as “… a full range of threats and hazards, including domestic terrorist attacks, natural and man-made disasters, accidental disruptions, and other emergencies” (p. 3).

- **Saboteur** – Disruption, destruction, or contamination; destroy public confidence in utility / government agency.
- **Insider** – Employees, vendors, delivery persons, consultants or contractors who engage in property damage, theft, disruption, destruction or contamination for revenge, financial gain, political causes or collusion with outsiders.[2]

Each classification of attacker has their own motivation factors, sophistication of attack, tools, weaponry, and levels of potential damage to a targeted site's assets. "Assets" typically include:

- **Physical:** Structures, vehicles, and their contents; equipment and supplies.
- **Information:** Hard-copied and digitized data; conventional files, computer networks and related equipment.
- **Human:** Employees and visitors.

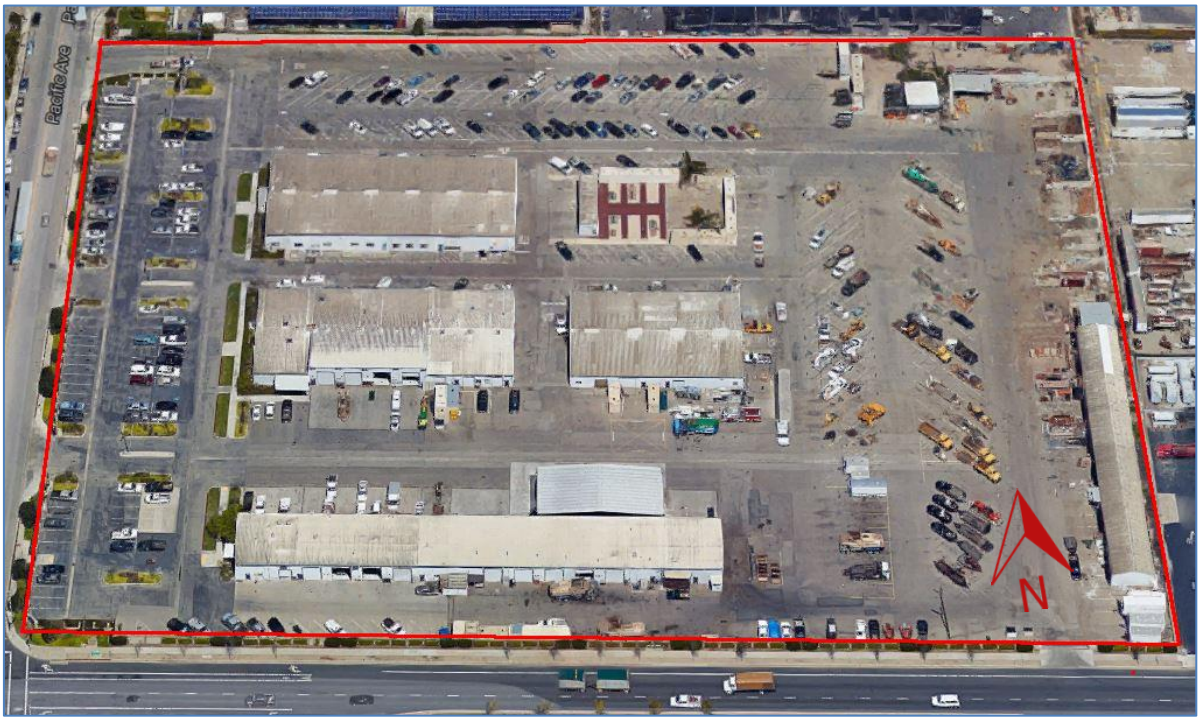


Figure 1. Maintenance Service Center perimeter in red (image courtesy of Google).

1.5 Local Crime Trends

The development of a physical security plan should include the evaluation of area criminal activity. Locations with higher crime rates typically justify enhanced security solutions based upon the propensity of area crime.

[2] Adapted from ANSI/ASCE/EWRI 56-10 and 57-10 (2011).

Summers Associates accessed crime data from the Oxnard Police Department's Crime Analysis Unit. In the 25-month period from January 2014 to February 2016, a total of 239 Part 1 crimes[3] were reported within a 0.5-mile radius of MSC.

Table 1. Known Offenses within 0.5-mile Radius of MSC, 01-01-2014 to 02-29-2016

Homicide	Rape	Robbery	Aggravated Assault	Burglary	Larceny	Motor Vehicle Theft	Arson
0	0	6	17	33	149	33	1

During this time frame, only one (1) Part 1 crime was reported on the MSC property—a burglary during late night/early morning hours in June 2014. The suspect/s cut chain link fencing to gain entry onto the property. Once on the property, shed door locks were cut and lawn equipment was taken. City management believes the suspect/s may have had some level of affiliation with the City; commonly known as an "inside job."

Additional pilferage of tools and equipment has occurred when employees fail to secure work vehicles. The dumping of hazardous waste on the property also occurs with some regularity.

According to the FBI's 2014 *Uniform Crime Reports*[4], Oxnard ranked 119 of 462 California cities in violent crime (74th percentile[5]) and 98 of 462 cities in property crime (79th percentile).

When comparative California cities are narrowed to between 100,000 and 300,000 population size, Oxnard (with its 2014 population listed at 204,159) does not fare much better. Out of 59 cities in the population range, Oxnard ranks 14th in violent crime (76th percentile) and 16th in property crime (73rd percentile).

Also concerning is the rise in Oxnard crime rates (see Table 2). As California generally enjoys declining crime rates over much of the past 30 years (see Figure 2), crime in Oxnard has increased steadily during the past five years with aggregated annual crime increases of nearly 83%, while its population has only increased about 2% during that same time.

[3] "Part 1 crimes" are defined by the FBI's *Uniform Crime Reporting* Program as: criminal homicide, rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson.

[4] 2014 is the latest annual UCR report available. See https://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2014/crime-in-the-u.s.-2014.

[5] For reference, the 50th percentile represents the city with an average comparative crime rate and the 100th percentile city has the highest crime rate among comparative cities.

Table 2. Known Offenses in Oxnard, 2011-2015							
Year	**Violent Crime**	**Robbery**	**Property Crime**	**Larceny-Theft**	**Aggravated Assault**	**Burglary**	**Annual Total**
2011	619	274	3,499	2,563	311	577	9,854
2012	603	304	4,071	2,677	282	848	10,797
2013	651	328	5,074	3,436	298	974	12,774
2014	884	447	6,409	4,475	381	1,172	15,782
2015[6]	920	383	6,720	4,758	502	1,103	14,386

In spite of criminal activity in the immediate area, decision-makers might wonder if there really is a security problem at MSC with just one (1) Part 1 crime reported in over two years. To focus only on property crimes would do a disservice to the City's most precious commodity: its employees.

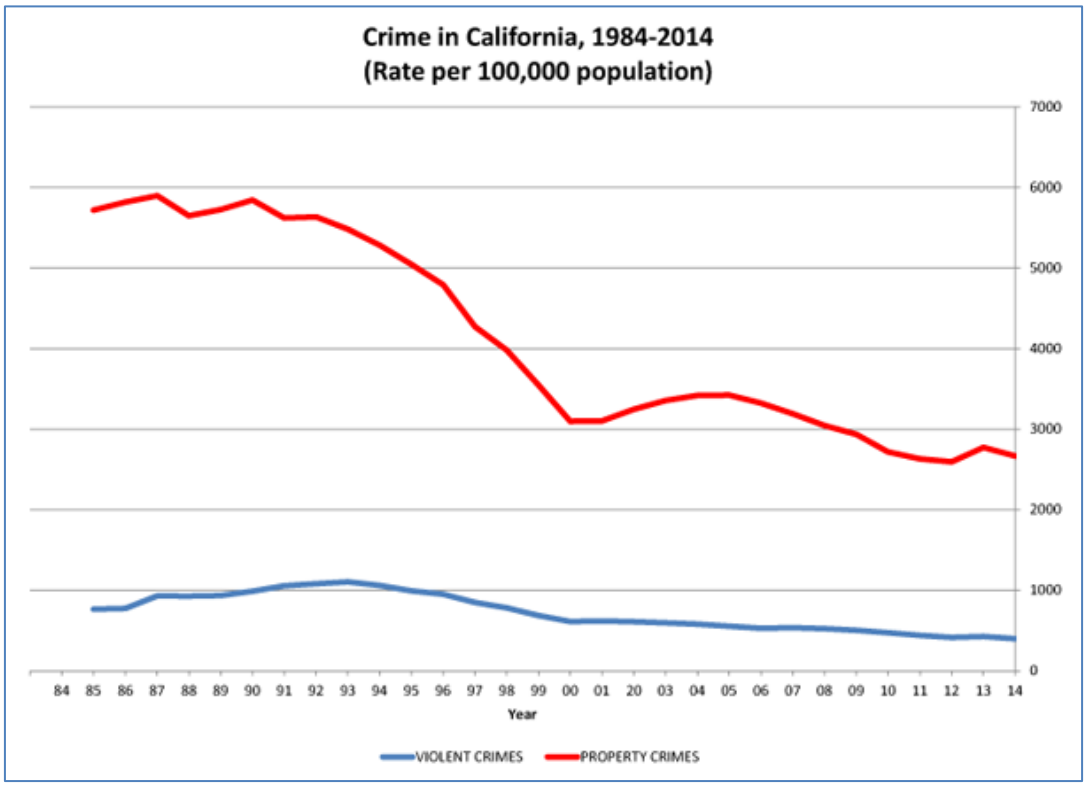


Figure 2. Courtesy of the California Office of the Attorney General.

Recent active shooter incidents—like that in San Bernardino—are stark reminders that soft government targets are at risk. One need only go so far as Oxnard City Hall and City Hall Annex to see that investment in target hardening strategies has become the norm in local government workplaces because local, county, state, and federal non-law

[6] 2015 crime data obtained from the Oxnard Police Department at https://www.oxnardpd.org/pressreleases/2894/.

enforcement-related government employees are nearly twice as likely to be the victim of a workplace violence incident.[7] Controlling workplace access is a primary physical security strategy.

1.6 Physical Security Systems

A properly designed physical security system accomplishes the following objectives:

- **Deterrence** – Makes target less accessible or attractive to attack. Typically accomplished by perimeter fencing, barriers, lighting, and/or electronic monitoring.
- **Detection** – Identifies unauthorized access to the protected property. Detection can by electronic means (alarms, cameras, etc.) or by employee or bystander observation.
- **Delay** – The slowing of an intruder's progress. Delaying an attack provides responders an opportunity to respond and address the incident in progress. Typically accomplished through the use of physical barriers.
- **Defend/Respond** – A physical security system is useless without a response component. This is typically law enforcement, private security personnel, or city employees who respond at the time of adversary detection to observe (i.e. evaluate an alarm activation to determine its veracity), report the intrusion to emergency responders, and/or respond by directly defending people or assets imperiled by the intruder/s. The level of response is based upon the individual's capacity, authority, equipment, and training.

The most common physical security design solution applied to minimize risk is the implementation of concentric layers of protection approach to a facility's design. Establishment of an outer perimeter, such as a fence or wall, serves as the first layer of defense. Hardened landscape or architectural features (reinforced sitting walls; planters; vehicle barriers) establish a second layer where possible; a hardened building shell typically serves as the second, or ideally third, layer of defense, followed by core asset space hardening and application of electronic and physical electronic security countermeasures as the third, or ideally fourth, layer of defense. Electronic security countermeasures are added to supplement the layered architectural approach to security; electronics are not implemented as a substitute for needed layers of protection.

As a general rule, the earlier threats/intrusions are detected, the greater the opportunities to protect assets and minimize the impact of losses and incidents. Threat detection, classification, assessment, and response, are critical to the overall performance of a properly designed and engineered security management program.

[7] Bureau of Justice Assistance. (2013). *Workplace violence against government employees, 1994-2011*.

1.7 Crime Prevention Through Environmental Design

Crime Prevention Through Environmental Design (CPTED) is a multi-disciplinary approach to deter criminal behavior through manipulation of the environment. Drawing heavily on behavioral science rather than target-hardening strategies, CPTED's fundamental premise is that the physical environment can be altered or managed to produce responses that reduces the incidence of crime. The goal of CPTED is the creation of an environment where legitimate users feel safe and secure, while potential criminals feel exposed and vulnerable. To achieve this goal, one should consider the following "Three Ds" of CPTED as related to existing facilities:

- **Designation**
  - What is the purpose of this space?
  - What was it originally intended to be used for?
  - How well does the space support its current use?

- **Definition**
  - How is the space defined?
  - Is it clear who owns it?
  - Where are its borders?
  - Are there social or cultural definitions that affect how the space is used?
  - Are there signs?
  - Is there a conflict or confusion between the designated purpose and definition?

- **Design**
  - How well does the physical design support the intended function?
  - How well does the physical design support the definition of the desired or accepted behavior?
  - Does the physical design conflict with the productive use of the space?

The four key elements of CPTED considered in this report's findings and recommendations are: natural surveillance, natural access control, territorial reinforcement, and order maintenance.

- **Natural Surveillance** – Maximizes line of sight opportunities and ensure that all areas within a designated environment are highly observable. Designs incorporating windows/fixed glass overlooking pedestrian pathways, stairways/stairwells, or gathering areas are highly encouraged. Natural surveillance is achieved by minimizing line-of-sight obstructions such as dense foliage, cluttered windows, or overbearing architectural features. Adequate lighting is another critical component supporting natural surveillance. Activities within an area that are well-lit and easy to observe enhance opportunities to see and be seen.

- **Natural Access Control** – Involves clarification of property boundaries along with the limitation of access routes into and out of a property. Natural access control is achieved through the manipulation of the natural environment which may include

the placement of trees; planters; sitting walls; boulders; hostile plants; monuments; and decorative art in such a manner as to guide, direct and or restrict pedestrian and or vehicular access or direction

- **Territorial Reinforcement** – Asserts ownership and control over an environment. Encourages the use of physical attributes that express ownership, such as fences, signage, art, logos, pavement treatment/pigmentation and landscaping.
- **Order Maintenance** – When an area deteriorates, the resulting decay attracts criminals. The decay provides an environment when their illicit activities will not stand out or attract undue attention; they fit right in. The lack of maintenance and care is interpreted as an abandonment of ownership. The perception of safety in these places is held only by perpetrators. Legitimate users of an environment feel safe only when that property is clean and aggressively maintained. This is an environment where criminals tend to feel out of place and highly vulnerable.

1.8 Lighting Standards

In determining the need for lighting, the *Illuminating Engineering Society of North America* (IESNA) in its publication IESNA G-10-3, "Guideline for Security Lighting for People, Property, and Public Spaces," describes the association between crime analysis and lighting systems necessity and design:

> The extent and type of lighting to be used as part of a balanced security system is determined by several factors. Critical among these is the actual criminal history on or near the property. An analysis of prior events and crime that have occurred on or around the site can help to establish the foreseeability of future crime at the location. For the professional security and lighting designer, or occupants of a particular site, foreseeability of crime should be considered in formulating the original security and safety lighting design, as well as planning for future needs. (p. 47)

The legal concept of *foreseeability* is particularly relevant in civil litigation and can be defined as "the facility to perceive, know if advance, or reasonably anticipate that damage or injury will probably ensue from acts or omissions."[8]

> In the law of Negligence, the foreseeability aspect of proximate cause—the event which is the primary cause of the injury—is established by proof that the actor, as a person of ordinary intelligence and circumspection, should reasonably have foreseen that his or her negligent act would imperil others, whether by the event that transpired or some similar

[8] Foreseeability. (n.d.) *West's Encyclopedia of American Law, edition 2*. (2008). Retrieved February 26 2016 from http://legal-dictionary.thefreedictionary.com/Foreseeability

> occurrence, and regardless of what the actor surmised would happen in regard to the actual event or the manner of causation of injuries.[9]

In a 2009 whitepaper entitled *Exterior Lighting for Energy Savings, Security, and Safety*[10], the U.S. Department of Energy (DOE) examined litigation issues with external lighting. These comments are worthy of full inclusion in this report as they deal directly with the topics of facility lighting levels and general maintenance:

> It is important to consider potential legal risks during facility design to address potential lawsuit situations. However, a lack of understanding of actual litigation experience related to exterior lighting can drive corporate policy to promote excessive light levels or other low efficiency elements as part of facility design. The same limited understanding of the drivers for litigation can also inhibit effective energy saving lighting retrofits. Therefore, an examination of what situations can trigger and eventually be successful in exterior lighting related litigation may help in avoiding roadblocks to effective energy savings applications.

A review of U.S. case law summaries related to exterior lighting shows that the critical issues prompting possible litigation were:

- Minimum illumination levels below the accepted industry standard for the specific application [the summary references illumination recommendations provided by IES (Illuminating Engineering Society) as the source of an appropriate standard for lighting].
- Illuminance insufficient for operation of security cameras [the summary generally relates this to non-uniform illumination].
- Lighting fixtures insufficiently safeguarded from vandalism.
- Lamps not inspected and sufficiently cleaned in high dirt accumulation conditions.
- Lamps not replaced before they burn out thereby creating non-uniform lighting conditions.
- Lack of notice by signage of any specific safety or security risk.

A summary conclusion from this representation of litigation issues is that all issues are based on negligence in meeting typical industry standards of care related to exterior lighting. The case law also general notes IES as providing this standard of care. The IES

[9] Ibid.

[10] Available online at: http://apps1.eere.energy.gov/buildings/publications/pdfs/alliances/exterior_lighting_savings.pdf

Handbook and associated related documents provide the recommended design practice that forms this collective standard. Lighting design that exceeds these recommendations is not shown to provide any specific additional protection from potential litigation. (p. 4)

DOE (2009) suggests that full-output lighting for most parking facilities is only necessary during business hours and only when users are accessing parking areas. The intended use of this facility may support such a functional option and should be considered by decision-makers. DOE also identifies LED (light-emitting diode) technology as a preferred option for parking area applications:

> LEDs provide potentially more uniform distribution, "whiter" light for better contrast and identification of objects, dimmability and instant on capability, and potentially longer useful life.
>
> Evaluate the use of parking areas and categorize as either:
>
> - Defined operating hours use (office, retail, maintenance/storage, etc.)
> - Potential intermittent 24/7 use (i.e., barracks, security)
>
> In defined hours of use facilities with known shift hours, apply time switching that will turn off most parking lot lighting after expected use of the parking area. This could be accomplished by time switching all but a few "night-lite" fixtures in the lot. It could also be accomplished by dimming the lot lighting after expected use hours (LEDs can be dimmed successfully).
>
> For expected intermittent use lighting, consider the use of lighting controlled by occupancy sensors. The sensors would activate part or all of the lot (depending on size) when occupants or vehicles approach or enter the area. This could be applied in place of dimming or switching in lots with defined use hours for afterhours use. (p. 5-6)

IESNA (G-1-03) defines four criteria to functionally describe lighting:

- *Illuminance* is the quantity of light that falls onto a surface.
- *Uniformity* is the evenness of light distribution on surfaces.
- *Glare* is caused by sources of light that are greater than the surrounding environment which adversely impacts visual performance and visibility.
- *Shadows* reduce the effectiveness of lighting and discourage a feeling of safety (pp. 6, 13).

Uniformity is a lighting criterion that is worthy of additional discussion. According to IESNA G-1-03:

Uniformity refers to the evenness of the distribution of light on the surface(s). In determining uniformity, minimum, average, and maximum illuminances are compared using ratios; either average-to-minimum or maximum-to-minimum. Uniformity in security lighting aids security perception, while reducing the necessity for eye adjustment when scanning or using the area. Uniformity ratios (average illuminance divided by minimum illuminance) vary depending upon the application. (p. 27)

IESNA G-1-03 has three guidelines for controlled spaces that are germaine to MSC because . They are:

Storage Yards, Industrial and Equipment Areas, and Container Terminals: Area lighting is typically accomplished with floodlighting or luminaires mounted on poles 9 m (30 ft) or more in height. The recommended average illuminance on the surface of large open areas is 5 to 20 lux (0.5 to 2 fc) with an average-to-minimum illuminance uniformity ratio not greater than 8:1. The greater the brightness of the surrounding area, the higher the illuminance required to balance the brightnesses in the space, while exercising caution to avoid light trespass and glare. Luminaire spacing will depend on the output, mounting height, and distribution of the luminaires. In storage areas where unacceptable material losses have been sustained, or security is an issue, the average maintained illuminance levels should be at least 10 lux (1fc), with an average-to-minimum uniformity ratio not greater than 6:1. (p. 22)

Parking Facilities (Lots and Garages): When security is an issue, the recommended security illuminance for open parking facilities should be an average of 30 lux (3 fc) on the pavement. A uniformity ratio not greater than 4:1, average-to-minimum should be maintained. Attention should be given to the use of the facility and hours of operation. Uniform lighting for an empty lot is of little value, but when space is used to capacity it is important to achieve the desired lighting level between vehicles since these are the likely places for crime to occur. (p.27)

Offices and Other Commercial Buildings (Exteriors): Primary points of entry to the building and the areas around these entrances should be easily visible and identifiable. Depending on the construction of the building, points of entry may include unintended entry points, such as through walls and roofs. Luminaires set in the ground, mounted on the building or under the eaves, or mounted on poles, provide light for these critical areas. While ground-mounted floodlights may provide uniform illuminance, they are accessible and can be readily neutralized. Pole-mounted luminaires are usually the best option for uniformly illuminating

the surfaces of the building and the surrounding area with less opportunity for vandalism. The average recommended vertical illuminance on the building façade ranges from 5 to 20 lux (0.5 to 2 fc) with a uniformity ratio no greater than 8:1 or 6:1 depending on the acceptability of losses.

PART II FINDINGS

The following observations were made by the assessment team and are based on meetings with key personnel and personal observations at MSC during daytime and nighttime hours. The observations are not listed in order of priority. The findings and recommendations are limited to the evaluation of the current state of physical security systems. If inadequate, recommendations are made to enhance the respective physical security system. Photographs are included to further illustrate the deficiency.

2.1 Property Perimeter

This 10-acre site is situated at the corner of a busy commercial district intersection. Its perimeter is defined by a combination of block walls, chain link and wrought iron fencing materials. There are four gated vehicle entry points; one pedestrian gate appears to be used for ADA accessibility and egress to the sidewalk along Pacific Avenue.

Figure 3. Compromised chain link fence on east side of MSC.

During business hours, all vehicle entry points are opened for regular use by City personnel. During the nighttime inspection, all entryways were closed and secured.

Chain link is considered an inferior fencing fabric for perimeter security purposes. It is easily defeated by climbing and—as evidenced in the MSC burglary—cutting. During the site inspection, two areas along the east fence were deficient and in need of immediate repair (see Figure 3).

Rolling vehicle gate entrances are equipped with electronic gate operator (Figure 4). Gate operators are either activated by a digital keypad or a radio I.D. device (Click2Enter®).

Figure 4. Rolling vehicle gate operator.

The combination block wall and metal fencing along Pacific Ave. (Figure 5) and part of Wooley Rd. is difficult—but not impossible—to scale. The open design offers motorists, pedestrians, and nearby businesses excellent natural surveillance opportunities onto the MSC property.

Figure 5. Combination block and metal fence bordering Pacific Ave.

The solid block walls along most of Wooley Rd. and the north side of MSC can be scaled with little difficulty (Figure 6). Vining plant materials on the wall along Wooley Rd. reduces the likelihood of graffiti-vandal attack. There are no natural surveillance opportunities with a solid wall, but visibility into protected property is not always a sound choice.

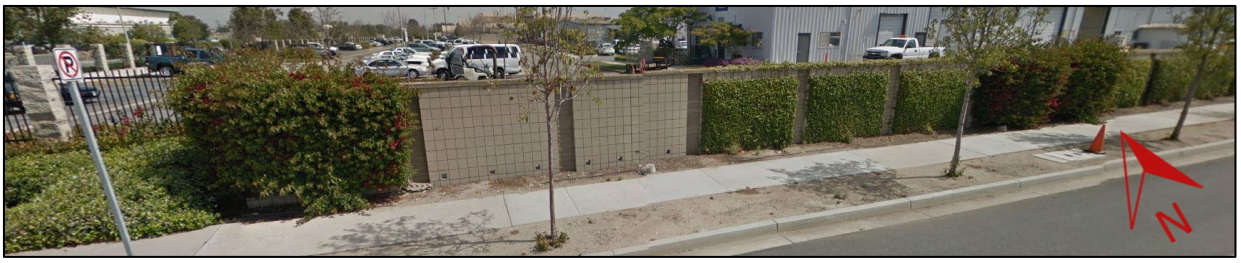


Figure 6. Wall bordering Wooley Rd. (courtesy of Google).

Signage can help differentiate what property is (a) open to the public, (b) semi-private and (c) private property or closed to public access. At the Wooley Rd. vehicle entrance, signage delineates a restricted access boundary (Figure 7). There is no such signage at any of the four Pacific Ave. entry points. Signage at these entry points included:

- Warning that the property is under video surveillance (the veracity of which is questionable and can be more of a liability than it is a successful crime prevention measure).
- No vehicle engine idling.
- Speed limit of 15 M.P.H.

Figure 7. Signage at the Wooley Rd. vehicle entrance (courtesy of Google).

2.2 Lighting Assessment

There is no property-wide lighting scheme at MSC. Three tall light poles—which may be associated with vehicle entry points along Pacific Ave. in the west parking area—seem to be the extent of any coordinated area lighting strategy. These lights offer a bright white light that is preferable in security applications and especially for video surveillance systems use, but the luminaires do not uniformly distribute light across the entire parking area, leaving the fringes underlit, as can be seen in the foreground of. Other areas of the MSC are illuminated by a variety of means, such as wall packs or other luminaires above doorways.

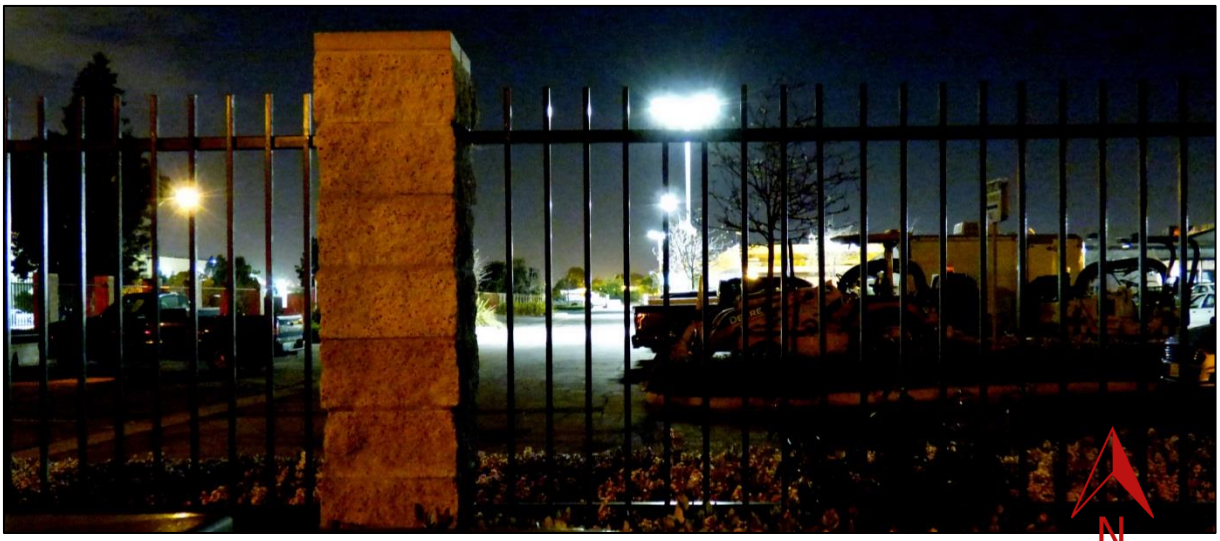


Figure 8. View of west parking lot lighting from Wooley Rd. to the north.

The property benefits slightly from spill lighting created by the commercial properties to the north and east, but as can be seen in Figure 9, lighting levels drop off to near-dark conditions near the center of the equipment storage lot on the east side of MSC.

Figure 9. Nighttime view along north wall of MSC.

There is little opportunity to casually observe the eastern parking and storage area during nighttime hours when the MSC is largely unoccupied by legitimate users (Figure 10).

Figure 10. View of eastern lot from Wooley Rd. vehicle gate.

2.3 Intrusion Detection (IDS)

Only Building #3 was noted to have a funtional intrusion detection system consisting of door contacts and back up interior motion detection protection. Evidence of previous era non functioning security equipment was noted in several areas.

IDS systems serve to minimize exposure to theft, vandalism and those associated with minimal to no key control management.

Figure 11. Unprotected window with equipment nearby.

2.4 Building / Facility Access Control

Employee access into MCS is controlled via a Linear keypad by entering a numeric code. Each employee is reportedly provided a code however no audits are ever conducted to see if former employee's codes or the same code is being utilized by others.

Figure 12. Employee Gate Keypad

The only access control to buildings are conventional doors and locks. Persons entering office spaces have unhindered access to interior office spaces after getting past a receptionist area, if one is present. The majority of door jams are exposed and vulnerable to tampering.

Figure 13. Exposed door jam with illustrated latch guard.

2.5 Video Surveillance

The only active video surveillance system at MSC is in the Napa contract auto parts distributor. The system consists of several interior cameras and one exterior fixed camera. Signage at MSC vehicle entries warn that the location is under video surveillance. Several exterior cameras at MSC are not functional and provide no forensic evidence value. The combination of a complete non-functioning video surveillance and contradictory signage may present liability containment exposures as the facility occasionally accessed by the general public.

2.6 Hazardous Materials Dumping

Near a shed that serves as a hazardous materials storage area, a large plastic yellow container is in place that is designed to contained discarded hazmat items. Unfortunately, this area has been a dumping place for various types of hazardous waste. Items are typically dumped on weekends when the MSC is closed. Because access to the facility cannot be tracked by individuals, and due to a complete lack of video surveillance at entrypoints or near the hazmat area, it is impossible to know who is leaving this waste at the facility. (See Figure 13).

Figure 14. Hazardous materials dumping area.

2.7 Asset Protection

During the site visit, various pieces of equipment were found unsecured in work areas. Keys to city-owned vehicles were found hanging on a board in an area that has no access control (Figure 15).


Figure 15. Key security in an unsecured area.

2.8 Emergency Egress

Pursuant to fire department regulations, the Conference Room in Building #2 must have two emergency exits. One exit feeds direclty into an employee office area. Because this constitutes an emergency exit, the door cannot be secured. The conference room is utilized by the general public occasionally.

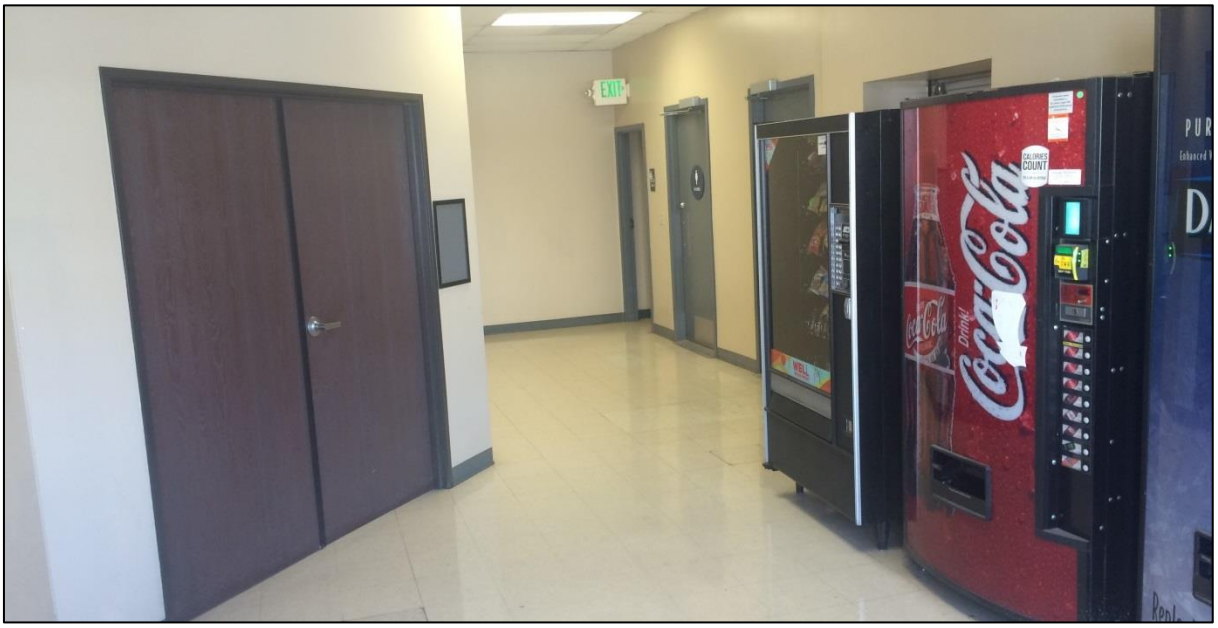


Figure 16. Conference Room and emergency exit.

The stacked files (Figure 16) noted in the Fleet Services hallway may present a fire life safety exposure from an emergency egress perspective particularly for a wheel chair. Concerns related to potential public access should also be reviewed.

Figure 17. Egress Obstruction

RECOMMENDATIONS

3.1 Property Perimeter

Recommendation: As a minimum, repairs should be made to the chain link fence along the MSC east perimeter to reestablish this outer most perimeter barrier. Because this remote area suffers from minimal natural surveillance line of site opportunities, it is the likely target for unauthorized entry attempts. Ideally, the chain link would be replaced to match either MSC's existing block wall or wrought iron fence for increased deterrence and consistency.

Estimated Cost: Requires further study.

Recommendation: Trash and discard equipment depicted in Figure 3 negatively impact the territorial reinforcement of this facility. Said items should be removed to resestablish the perception of territorial control to discourage unauthorized access.

Estimated Cost: Staff implemented.

3.2 Lighting

Recommendation: Continue the practice of converting all luminaires to white light (preferably LED). Since the incidence of crime within this neighborhood is minimal, consider future utilization of motion based LED lights at pedestrian and vehicle entry points for employees accessing the facility after hours. Light activation may also be integrated with the access control system.

Estimated Cost: Staff – future planning

3.3 Intrusion Detection (IDS)

Recommendation: All MSC buildings should be protected by a basic intrusion detection system consisting of all perimeter openings (doors & windows) supplemented by a secondary level of protection including dual technology motion detectors.

Each building should be equipped with its own IDS keypad for arming and disarming the system. Each building is considered its own independent system (AKA: "partitions") and the typical IDS system allows for up to 8 partitions within one IDS system. As a result, one intrusion detection system with multiple partitions should provide adequate protection from intrusion detection for MSC. Typical monthly monitoring charges from a UL Listed

central station are approximately $35 per month. The system should be programmed to arm automatically at a certain time each evening to minimize the exposure presented by employees forgetting to arm the system.

Estimated Cost: $5,000-$8,000 depending upon wired vs. hardwired configuration.

3.4 Access Control

Recommendation: The secondary fire door exit leading (Figure 16) into the Building 2 office area should be equipped with signage indicating “Emergency Exit Only – Alarm Will Sound” and a local key controlled annunciator unit to discourage unauthorized entry. This alternative is more cost effective than constructing a secondary door within the conference room.

Estimate Cost: $350.00

Recommendation: Request the authority having jurisdiction (AHJ) review the practice of stacking files within the Fleet Services hallway to ensure compliance with fire life safety codes. Furthermore, review potential public access to these files.

Estimated Cost: Staff

Recommendation: Access into the MSC should be controlled ideally by using the employee issued indentification badge which may also serve as an access control credential. Installation of a card readers at Employee Gates will track and control employee access. Eventually, card readers should be installed at all of the buildings employee entrances. This will eliminate the need to issue keys integrate the intrusion detetion into the access control system.

Estimated Cost: Staff – requires further study to develop rough order of magnitude cost. See Oxnard Utiliies Security Master Plan for guidance.

Recommendation: The unsecured key box seen in Figure 14 should be replaced with an card reader controlled unit which will maintain an inventory of all incoming and outgoing keys by employee. Employees will be required to use their identification / access control badge to access the unit.

Estimated Cost: $3,500

3.5 Video Surveillance

Recommendation: At a minimum, video surveillance coverage should be established to view and record all vehicle entry points. This should eliminate the occurrence of after-hours and or weekend illegal dumping at MSC. It also provides a visual audit trail of who enters the facility and when and may be compared against the Linear keypad audit trail or future card access control system to validate access is being granted to only current employees only. Secondarily, video surveillance cameras should be installed at the exterior of buildings to provide general activity recording of all facility egress points. This will discourage theft of tools from vehicles not secured by employees. 2.1 MP day / night cameras should be used and set to for motion based recording at not less than 15 frames per second with a 30 day minimum video retention programming set for the network video recorder.

Estimated Cost: $25,000-$30,000. See Oxnard Utilities Security Master Plan for guidance.

END OF REPORT

TABLE OF FIGURES

REFERENCES

American Society of Civil Engineers. (2011). *ANSI/ASCE/EWRI 57-10: Guidelines for the physical security of wastewater/stormwater facilities*. Restin, VA: Author.

American Society of Civil Engineers. (2011a). *ANSI/ASCE/EWRI 56-10: Guidelines for the physical security of water utilities*. Restin, VA: Author.

American Water Works Association. (2014). *Security practices for operations and management*. ANSI/AWWA G430-14. doi:10.12999/AWWA.G430.14

Bureau of Justice Assistance. (2013). *Workplace violence against government employees, 1994-2011.* National Crime Victimization Survey. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4615

Illuminating Engineering Society of North America. (2003). *Guideline for security lighting for people, property, and public spaces*.

U.S. Department of Energy. (2009). *Exterior lighting for energy savings, security, and safety*. http://apps1.eere.energy.gov/buildings/publications/pdfs/alliances/exterior_lighting_savings.pdf