City of Riverside
Regional Water Quality Control Plant
Security Assessment Study

SECURITY ASSESSMENT STUDY

FINAL | January 2023

City of Riverside
Regional Water Quality Control Plant
Security Assessment Study

SECURITY ASSESSMENT STUDY

FINAL | January 2023

Contents

Appendices

Tables

Figures

Abbreviations

ACS	access control system
ANSI	American National Standards Institute
ANSI 57-10	ANSI/ASCE/EWRI 57-10 Standard Guidelines for Physical Security of Wastewater/Stormwater Utilities
ASCE	American Society of Civil Engineers
AWWA	American Water Works Association
CAP	Crimes Against Persons/Property
Carollo	Carollo Engineers, Inc.
CCTV	closed-circuit television
CIP	Capital Improvement Program
City	City of Riverside
CPTED	Criminal Prevention Through Environmental Design
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
EWRI	Environmental & Water Resources Institute
FBI	Federal Bureau of Investigation
FTE	full-time equivalent
IDS	intrusion detection system
IEDs	improvised explosive devices
IIDs	ignition interlock devices
MCC	motor control center
RWQCP	Regional Water Quality Control Plant
SCADA	supervisory control and data acquisition
TM	technical memorandum

Section 1

EXECUTIVE SUMMARY

The City of Riverside (City) has experienced increased criminal activity at its Regional Water Quality Control Plant (RWQCP) over the last several years, including breaking and entering, theft, simple assault, and vandalism. These incidents have become a significant safety threat and concern to plant staff and operations. The purpose of this report is to assess the existing level of security at the RWQCP and provide recommendations for future Capital Improvement Program (CIP) projects to close the gap between the current and desired security conditions.

Members of the assessment team visited the RWQCP on July 13, 2022 and August 17, 2022 to evaluate the RWQCP's existing security measures and gather information related to the security planning process. These site evaluations were completed using the concept of layered security to assess the RWQCP's perimeter (Layer 1), clear zone (Layer 2), building (Layer 3), sitewide (Layer 4), and operational (Layer 5) security. Information collected during these site visits, discussions with RWQCP personnel, and analysis of the threat environment were used to assess the RWQCP's current level of security and compare it to the American National Standards Institute (ANSI)/American Society of Civil Engineers (ASCE)/Environmental & Water Resources Institute (EWRI) 57-10 Standard Guidelines for Physical Security of Wastewater/Stormwater Utilities (ANSI 57-10) and industry best practices for physical, electronic, and operational security.

The RWQCP meets or partially meets many components of ANSI 57-10 and general security best practices, including components of perimeter fencing, physical equipment protection, door locking, and backup power. However, there are several security measures that the RWQCP should address to fully meet the standards and improve plant operations safety including the addition of alarm assessment, intrusion detection, system monitoring, security specific closed-circuit television (CCTV), and updated security policies and procedures. A detailed discussion of existing conditions at the RWQCP relative to ANSI 57-10 and security best practices is provided in Section 5 for each level of security.

The security assessment generated a list of recommendations to address identified deficiencies and improve the overall security profile of the RWQCP. The complete list of recommendations is presented in Section 6 of this report and includes a reference to the applicable ANSI 57-10 guideline, as well as the relative priority, and estimated implementation cost of each recommendation. The recommendations were organized into seven security projects based on the scope and priority of each item.

Table ES.1 includes a planning level cost overview and recommended implementation schedule for each security project. In general, projects recommended for short-term implementation include high priority or low cost work items that can significantly improve the RWQCP security profile. An itemized breakdown of the costs associated with each recommendation and project is included in Appendix D. Note that these planning level costs represent high-level budgetary estimates based on Carollo Engineers, Inc. (Carollo's) understanding of the design effort and

implementation costs required at the project location. The preliminary costs will be further refined based on the ultimate project details and market conditions during the design phase of each project.

The anticipated cost to implement all of the security projects and recommendations is $3,994,500. This cost includes 1 year of interim mobile CCTV units, as recommended later in this study and detailed further within Appendix C. This number will change based on the actual mobile CCTV usage timeframe (pending implementation of Project 2). Project implementation can be completed in phases over several years to improve the security profile at the RWQCP and assist in meeting ANSI 57-10 guidelines and best practice recommendations. The projects listed in Table ES.1 have been presented based on their proposed implementation timeline. As noted above, the interim security improvements project is recommended for immediate implementation until a permanent CCTV perimeter protection system can be installed as part of Project 2.

Table ES.1 Security Project Implementation Summary

Implementation Schedule	Project	Project Cost[1][2]
Present	Interim Security Improvements – Mobile CCTV	$254,500[3]
2023	Project 7 - Miscellaneous Electrical Security Upgrades	$20,000
2023	Project 5 - Security Policy and Procedures	$50,000
2023-2024	Project 2 - CCTV Perimeter Protection	$2,340,000
2024-2025	Project 4 - Access Control and Intrusion Detection	$790,000
2025	Project 1 - Plant Fencing and CPTED Improvements	$220,000
2025	Project 3 - Internal Surveillance/IDS with Video	$200,000
2025	Project 6 - Miscellaneous Physical Security Upgrades	$120,000
	TOTAL	**$3,994,500[4]**

Notes:
(1) Costs are based on October 2022 market conditions and include the following: 30 percent contingency, 9.5 percent taxes, 30 percent Engineering/Admin Fees, 18 percent Contractor's Overhead and Profit. Escalation to mid-point of construction has not been included.
(2) The project costs were rounded up to the nearest $10,000.
(3) Approximate cost for interim CCTV solution is for one year of mobile CCTV units, based on a monthly operating cost of $21,210 as provided by ECAMSECURE. Actual cost could be less or more depending on completion of Project 2, which will supersede the interim mobile CCTV solution. Refer to Appendix C for more details.
(4) As noted above, total implementation costs include 1 year of interim mobile CCTV units. This number will change based on actual mobile CCTV timeframe (pending implementation of Project 2).

Section 2

INTRODUCTION

The RWQCP is owned and operated by the City Public Works Department Sewer Division and is located on approximately 100 acres of land adjacent to the Santa Ana River in Riverside, California. The plant is a critical asset as it treats all of the wastewater flow generated within the City (equivalent to an average of 27 million gallons per day). Therefore, the facility requires a high level of protection.

Over the last several years, the City has experienced an increased number of break-ins and thefts at the RWQCP site, particularly at night. The presence of unauthorized individuals on plant grounds is a significant safety and liability concern for plant staff and operations. To address these concerns, the City hired Carollo to develop a comprehensive security assessment designed to identify and reduce the security risks associated with the facility.

2.1 Purpose

The purpose of this document is to assess the existing level of security at the RWQCP and provide recommendations for future CIP projects to close the gap between the current and desired security conditions. This assessment includes an evaluation of the RWQCP threat environment, followed by a review of the current site security controls. Current conditions were then measured against ANSI/ASCE/EWRI 57-10 Standard Guidelines for Physical Security of Wastewater/Stormwater Utilities (ANSI 57-10). This guideline is an ASCE standard which has been developed with the support of the American Water Works Association (AWWA) and the Department of Homeland Security (DHS) to assist utilities in achieving a level of security commensurate with threats to the sector. The current conditions were also evaluated against industry best practices for physical, electronic, and operational security.

2.2 Team

The security assessment team consisted of individuals from Carollo and the City. The Carollo team provided expertise in wastewater engineering, security planning and design, and risk management. Members of the City played a crucial role in contributing institutional knowledge and local experience associated with their system throughout the assessment process. The teams were comprised of the following individuals:

- City team:
  - Edward Filadelfia: Deputy Public Works Director - Wastewater System.
  - Ernest Marquez: Principal Engineer.
  - Elaine Radke: Senior Engineer.
  - John Koenig: Safety Officer.
  - Robert Eland: Operations Manager.
  - Bryan Padilla: Chief Plant Operator.
  - Brent Keaster: Maintenance Manager.

- Carollo team:
  - Graham Juby: Principal-in-Charge.
  - Dave Sobeck: Project Manager.
  - George Whitten: Assistant Project Manager/Project Engineer.
  - Kim Shust: Security Engineer.
  - John Saunders: Security Subject Matter Expert.

Section 3

METHODOLOGY

This section summarizes the methodology used to perform the security assessment.

3.1 Report Organization

Evaluation of an organization's security profile requires a comprehensive understanding of security best practices and the overall security goals of that organization. The methodology used to complete the RWQCP security assessment is detailed in the steps below:

- Evaluation of the RWQCP threat environment (who or what the threat is, what the objectives or goals of an attacker are, and what tactics can be expected).
- Benchmarking of the RWQCP site against the security recommendations outlined in ANSI 57-10.
- Detailed assessment of the existing RWQCP security profile, including:
  - A discussion of security best practices for each security element.
  - An assessment of each security element as it relates to the RWQCP site and City organization.
  - A review of the ANSI 57-10 guidelines.
  - A comparison against industry best practices for physical, electronic, and operational security.
  - A prioritized list of recommendations to address the perceived security vulnerability, including a high-level cost for each set of recommendations.

3.2 Security Approach

All security must be purposeful and have well-defined objectives. In its simplest form, security is intended to achieve three fundamental objectives:

1. Increase the level of effort needed to commit a crime.
2. Increase the risk that a criminal will be caught.
3. Reduce the rewards a criminal receives from committing a crime.

The mitigation recommendations outlined within this report were developed with these objectives in mind. The objectives are further defined in the following subsections.

3.2.1 Increase the Effort Needed to Commit a Crime

Work ratio is the relationship between effort and reward. If the relative cost or required effort to execute an attack is too high (i.e., high work ratio), the attacker will likely look elsewhere to commit the crime. In this context, work ratio is essentially a level of deterrence. There are several ways that a security program can make this ratio unmanageable or undesirable for an attacker.

Physical impediments such as high-level security locks, pry-guards on doors, wire mesh between sheetrock layers, security-screened windows and vents, welded hinges, and high walls/fences can serve to harden a target. While these security efforts may be supplemented by electronic

devices for monitoring and detection, they can and should stand on their own as highly effective security measures. In addition, guard services are often an essential tool in a security profile. To escape detection during a crime, an intruder must avoid other individuals on the site - including security personnel.

3.2.2 Increase the Risk of Being Caught

Although there are obvious exceptions, an attacker typically does not want to get caught while committing a criminal act. If the attacker is aware of an increased risk of being caught, they are more likely to be deterred from committing that act. A variety of strategies can be employed to increase the risk of being caught.

CPTED is a strategy that relies on maximizing sight lines at a facility and minimizing hiding places for criminals. The use of CCTV systems is also a very effective method of raising the risk of being caught. A CCTV system can provide extremely useful information to monitoring and response personnel when a security breach occurs. Rapid and informed response is fundamental to raising the risk level for criminals.

Another tool for increasing the risk of being caught is adequate site lighting. Site lighting can also serve to improve general staff safety. With this in mind, members of the assessment team visited the RWQCP site on August 17, 2022 to collect light intensity data. The data was designed to identify supplementary lighting needs to support plant operations and staff safety. The findings of the study are provided in Appendix A and are integrated into the results and recommendations provided in Section 5.

Badging or other identification procedures can also serve as a deterrent to criminals. The objective of a badging program is to make it obvious who is authorized to be on site and who is not, and to make those who are not authorized stand out.

Finally, guard services can also provide a visible deterrent to help prevent criminal activity, as well as the ability to quickly respond to any intrusions. However, such a service can be extremely costly – ranging from $150K - $250K annually for a single full-time equivalent (FTE) – and is not always within the financial means of a utility. While having a guard on site can provide a deterrent effect, that deterrent is typically only manifested in areas that the guard is seen. A site as large as the RWQCP cannot be effectively patrolled by a single guard and potential intruders would be able to determine where the guard is at any time and circumvent their patrols.

The ideal security approach includes a combination of guard service and perimeter and interior detection. This allows the electronic component of security (typically the CCTV system) to identify breaches and provide information to the guards to respond. This local guard response will always be quicker than an off-site (police or otherwise) response protocol. However, as this approach is not always viable due to the associated costs, the next best option is an effective perimeter protection system, integrated with an effective interior protection system, with detailed monitoring and response protocols based on the information that is provided by these systems. While the capital costs for this approach can be higher, the level of security provided is extensive and annual operating costs are far less than associated with a full-time guard service.

Ultimately, the single best tool to raise the risk to a criminal is awareness training for on-site personnel. The development of response and monitoring protocols are part of the recommendations detailed in the report.

3.2.3 Reduce the Reward Associated with Committing a Crime

An attacker has a specific goal in mind. If the value of an attacker's target is reduced, such that the attacker's goal cannot be obtained, it could deter the attacker. Staff should work to reduce obvious targets, such as a computer beside a window or an unlocked car with the keys in the ignition.

3.3 Security Planning

The security planning process can be summarized as follows:

1. What is being protected?
    a. This is an assessment of an organization's assets, and how important each asset is in achieving the organization's mission.
2. What (or who) are we protecting against?
    a. This is an analysis of the threats facing an organization, ranging from local level threats to international terrorist level threats. This report addresses the potential attacker's goals, threat vectors, and tactics relative to the RWQCP's assets.
3. How is protection provided?
    a. This is an analysis and review of the physical, electronic, and operational security measures currently in place to protect assets.
4. What is the gap?
    a. Analysis of the first three questions will demonstrate the vulnerabilities in the current security profile. This report includes discussions of the best practices and standards to apply to the RWQCP security program. Security planning addresses how to close the gap that is identified in answering these questions.

Figure 1 illustrates the security planning process in its entirety, including identification of critical assets, assessment of threats, evaluation of existing security processes, and analysis of gaps. The resulting plan provides a blueprint to use in developing and implementing an effective security strategy.

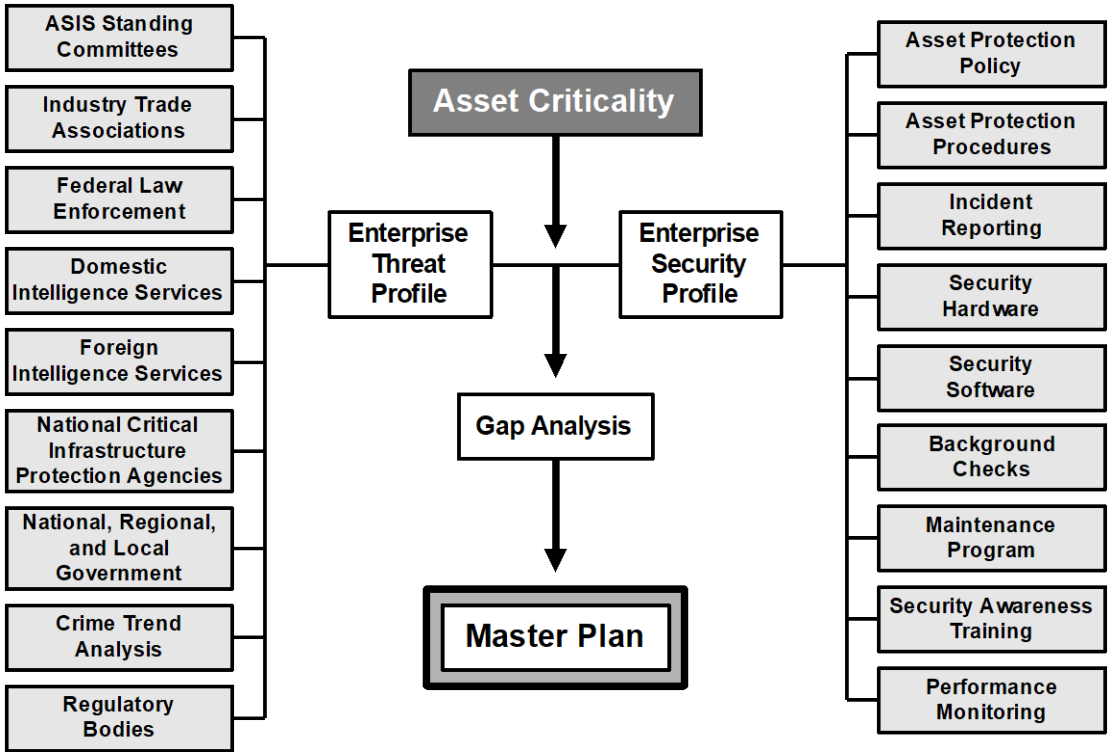

Figure 1 Security Planning Process

3.3.1 Site Evaluation

Site visits were completed on July 13th, 2022 to evaluate the RWQCP's existing security measures and gather information on the four security planning questions noted above. A site evaluation uses the lens of layered security to achieve the most comprehensive results. The concept of layered security is widely accepted within the physical and cybersecurity industries. The intent of a security program is to deter, detect, delay, and respond to troublesome events. An effective security program will establish concentric layers of security that must be overcome prior to an attacker causing undesired consequences.

- Layer 1 (L1) includes the perimeter of the site.
- Layer 2 (L2) includes the clear zone between the perimeter and any buildings. This layer also includes hatches, pump/lift stations, and outdoor equipment.
- Layer 3 (L3) includes the building envelope, including doors, gates, walls, and windows.
- Layer 4 (L4) includes the interior of buildings, as well as sitewide security. Sitewide security consists of controls or elements which can and should be viewed in a more holistic manner, since they are relevant throughout the site.
- Layer 5 (L5) includes the various security related policies and procedures that should be evident within an organization. These procedures include how visitors and contractors are handled, security awareness training, and background checks. Most of the Layer 5 features are not included in ANSI 57-10 but are often the most effective way to rapidly enhance the security profile of an organization and gain the most benefit from implementation of the previous four layers of security.

The approach outlined above is consistent with the ANSI 57-10 assessment approach. While ANSI 57-10 does not specifically mention layers, the recommendations use specific terms that directly correspond to the layers of security, as illustrated in Table 1.

Table 1 ANSI 57-10 Guidelines and Layers of Security Terminology

ANSI 57-10 Guideline Reference Language	Layer Reference
Fencing Perimeter and Walls	Layer 1
Gates	Layer 1
Site Areas	Layer 2
Facility Entrances	Layer 1
Bollards and Vehicle Barriers	Layers 1 & 2
Exterior Surfaces	Layer 2
Outdoor Security Lighting	Layers 1 & 2
Signage	Layers 1 & 2
Electronic Security Systems	All Layers
Access Control Systems (ACS)	All Layers
CCTV Systems	All Layers
Security Controls and Wiring	All Layers
Building Elements	Layer 3
Hatches, Vaults, and Vents	Layers 2 & 3
Online Water Quality Monitoring	Layer 4
Operator Devices	Layer 4
Chemical Fill Line Locking	Layer 4
Manholes	Layer 2

Section 4

THREAT PROFILE

4.1 General

This section outlines possible threats to the RWQCP. The following foundational elements are key to achieving a better understanding of these potential threats.

First and foremost, a threat is rarely, if ever, truly identifiable. The ways an intruder might damage a facility (i.e., vulnerabilities) and the methods to counteract those vulnerabilities effectively (i.e., security programs) can be assessed with a high degree of accuracy. However, it is very difficult to know with complete accuracy when, where, how, and if an attack will occur.

Second, individuals outside the water and wastewater sector typically have little knowledge of the most viable targets within a water or wastewater facility. Whereas most attackers would not be able to distinguish between a water and a wastewater facility, or between a critical asset and a non-critical asset, an industry or organization insider would have specific knowledge of targets and techniques. Consequently, it is important to consider that an insider, or an attacker colluding with an insider, would provide a more specific, more viable, and potentially more significant threat to the facility.

The information outlined in the following sections is based on site specific data, industry intelligence, and information provided by employees and facility management with knowledge of operations and experience in security situations.

4.2 Design Basis Threat

The ANSI 57-10 Standard references the Design Basis Threat to help identify specific types of adversaries, including their motivation, available equipment, and weapons. The approach was originally developed shortly after September 11, 2001 when most of the nation's security efforts were focused on preventing international terrorism. It is possible that this led to an overly conservative approach to security by essentially designing security to prevent the worst possible malevolent attacker - an international terrorist team with access to extensive equipment and weapons.

The reality is that the possibility of such an attack is small, with an estimated likelihood of 10^{-6} per the Environmental Protection Agency (EPA). Consequently, using the Design Basis Threat worst-case methodology could lead to identification of security recommendations that may not be commensurate with the real issues facing a facility.

More recent industry efforts have focused instead on preventing the worst reasonable case. The recommendations provided in this study consider security best practices, as applied to the most likely threats to the RWQCP facility.

4.3 Water and Wastewater Threats

Properly treating wastewater is vital for preventing disease and protecting the environment. The 16,000 publicly owned wastewater systems in the United States play a critical role in protecting the health of over 75 percent of the country's population. From a security perspective, the water and wastewater sectors are treated similarly by the EPA and the DHS.

Water and wastewater systems are vulnerable to both manmade and natural threats, including earthquakes, flood, droughts, malevolent attacks, contamination, and cyber-attacks. Any incident that negatively affects the wastewater system would have far-reaching public health, economic, environmental, and psychological impacts. Loss of these critical services could result in significant consequences to the national or regional economy. Assessing the security and risk of such systems is critically important.

The most prominent attacks on wastewater systems include:

- Service disruptions or loss of an asset from malevolent attacks such as terrorism, theft, sabotage, or vandalism.
- Breaches in cybersecurity.
- Introduction of chemicals or other foreign matter that affect the treatment process and limit the ability to effectively treat wastewater.
- Sabotage of equipment such as pumps and valves, which could lead to long-term disruptions to system flow and treatment.

The wastewater sector is complex, composed of infrastructure of varying sizes and types of ownership. The sector has unique risks that drive sector security and resilience activities, including various threats, vulnerabilities, and consequences.

In addition, many attackers are unable to differentiate between water and wastewater facilities, leading to similar consequences in terms of human loss and impacts. As a result, emergency response planning is essential to the sector to ensure continuity of operations and to sustain public health and environmental protection.

4.3.1 Vulnerabilities and Other Challenges in the United States

As previously noted, an attack on a wastewater system can take a variety of forms due to the complexity of the processes involved.

Wastewater treatment plants: In most cases, the wastewater treatment plant constitutes the last barrier between effective control of wastewater and damage to the environment. Often this is also the last place that a utility can continuously control the chemical and physical characteristics of the collected and treated wastewater.

Lift stations: These facilities are often constructed in locations with limited space and can benefit significantly from even a moderate level of physical security. Lift stations can be located in more remote areas and are sometimes widely dispersed, often resulting in inadequate security systems and associated monitoring. In the event of a lift station failure, caused by a force main break, power outage, or pump failure, wastewater may collect in the lift station wet well and back up into the collection system. This can result in environmental damage as well as danger to human health.

Collection system: The collection system is generally the most vulnerable part of a wastewater system given the general lack of security or monitoring. As a result, the most likely scenario for an attack on the wastewater system is damage the collection system, which can cause sewer overflows within the utility.

4.3.2 Previous Water and Wastewater Sector Attacks

The water and wastewater sectors have seen an increasing number of attacks in recent years. Table 2 provides a list of recent incidents. Most recently in July 2022, an unauthorized individual, currently designated as a possible saboteur, illegally gained access to a wastewater facility in Southern California and attempted to cause a major spill that would have flooded the plant and created a massive hazard to public health. The DHS intelligence report on this matter adjudged it to be a "... deliberative, targeted effort to sabotage the facility rather than just an act of random vandalism." The person tailgated into the site (entering after an employee opened the gate) and proceeded to break into several buildings unprotected by security technology or strong physical security elements. The individual was able to cut electrical lines, access and manipulate pumps and valves, and turn off some processes. This attack could have had much larger consequences, if not for the alert actions of employees on site. It also demonstrates that such an attack can happen to any organization and that each facility must take actions to prevent such an occurrence.

Table 2 Recent Attacks on Water and Wastewater Systems

Year	Incident Report
2002	In Rome, Italy, four men of the Salafist Group for Preaching and Combat were arrested in possession of chemicals, false papers, and detailed plans for the water supply network in the zone of the Embassy of the United States.
2002	Two Al-Qaeda agents were arrested in Denver with plans to poison water resources.
2004	The Federal Bureau of Investigation (FBI) and the DHS issued a bulletin warning that terrorists were trying to recruit employees from water treatment plants as part of a drinking water poisoning project.
2006	A water tank in Tring, England was deliberately contaminated with herbicide.
2006	Strychnine (a pesticide) was intentionally released into a Danish artificial lake.
2007	In China, 201 people died from using water intentionally contaminated with fluoroacetamide (a pesticide).
2008	In Varney, Virginia, a man was arrested in possession of two vials of cyanide intended to poison the water supply system.
2008	The water supply system of a Burmese refugee camp in Thailand (with a population of 30,000) was intentionally poisoned with herbicide.
2009	In the Philippines, the Frente Moro de Liberación Islámica (MILF) poisoned sources of water used by government soldiers and the population.
2010	In England, two neo-Nazis (a father and son) were convicted of several counts of terrorism, including castor-making and conspiracy with Serbian Nazis to poison water resources used by Muslims.
2011	Documents seized during Operation Neptune Spear (which led to the death of Osama bin Laden) revealed plans for poisoning US water resources.
2011	In Spain (La Línea de la Concepción, Cadiz), a conspiracy to poison water resources in response to the death of Osama bin Laden was thwarted.

Year	Incident Report
2012	In Australia, two 5,000-liter drinking water tanks were deliberately poisoned with Diuron (an herbicide).
2012	In Afghanistan, hundreds of girls in a school fell ill after deliberate poisoning of the water supply system.
2019	A former employee of the Post Rock Water District in Kansas was able to remotely access one of the Post Rock Water District computers to shut down potable water treatment and disinfecting systems.
2021	The City of Oldsmar, Florida suffered a cyberattack during which the attacker attempted to poison the drinking water with toxic amounts of sodium hydroxide.
2021	Multiple ransomware and remote access attacks targeting water utilities information technology systems including California (3x), Maryland, Maine, Pennsylvania, Nevada, Florida.
2022	Southern California Wastewater Treatment Plant illegally entered with an attempt to create spillage and environmental and process damage.
2023	Sabotage of transformer equipment (by way of shooting) at several substations in Moore County, North Carolina leading to mass blackouts affecting neighboring utilities.

4.4 Crimes Against Persons/Property (CAP) Index Statistical Evaluation

The Crimes Against Persons/Property (CAP) Index is another tool that can be applied to criminal risk analysis. The CAP methodology provides an analysis and likelihood forecast of a particular location's risk of exposure to crime. The analysis is not just a reflection of crime rates for a particular area - it also considers a wide range of demographic characteristics that dispose an area to criminal activity. The data reflects the relationship between crime and social disorganization.

The CAP Index model evaluates approximately 150 demographic variables, as well as numerous sources of historical reported crime. Some of the demographic variables accounted for by the model include:

- Population data.
- Housing data.
- Rental data.
- Population mobility.
- Economic data.
- Education data.
- Transience data.
- Marital status.
- Employment rates.
- Transportation methods.
- Travel time to work.

The CAP Index report uses Crimecast scores, which contextualize a location's crime risk in relation to the rest of the country. Scores can range from 0 to 2,000 and represent a relative probability, with 0 representing the lowest crime risk, 100 representing average crime risk, and 2,000 representing the highest crime risk. For example, a national score of 100 signifies a crime

risk in a given location is equal to the national average, a score of 600 indicates a crime risk six times higher than the national average, and a score of 25 denotes a crime risk a quarter of the national average.

Crimecast scores are normally reported for seven types of crimes: homicide, sexual assault, robbery, aggravated assault, breaking and entering, theft, and motor vehicle theft. Based on discussions with RWQCP personnel, simple assault and vandalism were also included in the evaluation since they are of notable concern. The Index provides a score for overall CAP, using the scores for burglary, larceny, and motor vehicle theft; and an overall CAP Index, which is a weighted average of the homicide, sexual assault, and robbery scores (leaning heavily towards the robbery criteria). The three types of crimes used for the CAP Index number are those that pose the greatest danger to individuals in an operational environment.

In the CAP Index model, the score for each census tract is calculated based on characteristics that are internal to that tract, with no influence from other nearby tracts.

The CAP Index report includes a three-mile radius map that displays CAP Index scores for the area surrounding the facility, indicated by census tract. For the purposes of this assessment, the one-mile radius map for the RWQCP facility was used. The one-mile view more directly reflects the immediate risk and is less influenced by crime that takes place a greater distance from the facility.

The CAP Index report also provides address-specific data, utilizing block level data on the legal inhabitants surrounding the address and the level of social disorganization. The data is then rolled up into the census tract boundary for ease of viewing.

The CAP Index score and the one-mile radius CAP index map for the RWQCP site are provided in Figure 2 and Figure 3, respectively.

Figure 2 RWQCP CAP Index Score

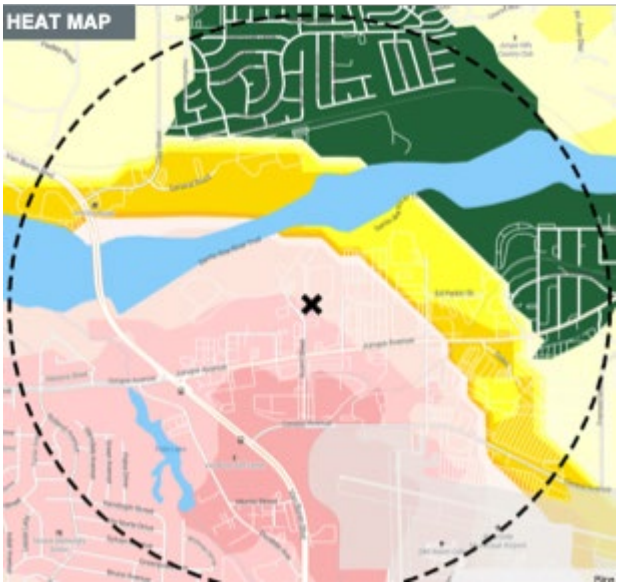

Figure 3 RWQCP One-Mile Radius CAP Index Map

The national CAP Index score for the RWQCP is reported as 280. This indicates that violent crime in the immediate area is almost three times the national average.

The color coding included as part of the CAP Index makes it easy to assess the risk in an area. Green areas represent the lowest risk (below the national average), yellow areas represent moderate risk, and the various shades of red and darker red indicate increased risk.

It is apparent that the higher crime areas to the south and west are affecting the potential risk at the RWQCP. It is important to understand that crime has an element of mobility - if police focus on high crime areas, making a strong show of force in the area west of the RWQCP, it would not be unusual for the current crime in that area to drift to locations where there is less law enforcement presence.

4.4.1 Crimecast Scoring

The CAP Index report also provides a set of Crimecast scores that are specific to a site, and represent the site's overall risk. This set of scores is not simply equal to the set of scores for the census tract in which the site is located. It is a weighted average of scores for tracts within a given radius of the site. The CAP Index model uses a radius threshold analysis to determine a site's overall risk, i.e. the site-specific Crimecast scores.

Because an address specific score is related to weighted tracts around the area, it is possible for a site to be located in a census tract with low crime risk but have an overall site crime risk that is much higher.

The Crimecast scores for the RWQCP are provided in Table 3. The national scores provide the site's risk in comparison to all 50 states and the District of Columbia broken down by crime category, while the California Scores compare the site to state averages and the Riverside County Scores compare them to County averages. Past, current, and projected risk scores are also provided to support trend analysis.

Table 3 RWQCP Crimecast Scores

	United States			California			Riverside County		
	Past 2010	Current 2022	Projected 2027	Past 2010	Current 2022	Projected 2027	Past 2010	Current 2022	Projected 2027
Cap Index Score	**352**	**280**	**282**	**259**	**216**	**220**	**237**	**201**	**197**
Crimes Against Persons	**323**	**281**	**260**	**244**	**223**	**208**	**198**	**175**	**160**
Homicide	180	218	227	179	224	230	148	180	175
Sexual Assault	378	328	274	304	332	288	191	207	174
Robbery	353	278	287	252	201	209	255	205	205
Aggravated Assault	306	282	252	234	227	205	178	162	144
Crimes Against Property	**418**	**294**	**289**	**332**	**252**	**253**	**257**	**206**	**202**
Burglary	308	218	219	278	211	215	190	164	165
Larceny	422	291	281	348	263	259	276	217	211
Motor Vehicle Theft	636	530	535	359	303	317	292	251	246
Crimes of Concern at RWQCP									
Assault	384	319	251	298	300	240	179	177	144
Vandalism	375	233	195	352	258	221	214	168	144

The results in Table 3 confirm that crime is a serious concern at the RWQCP. There are no crimes or collection of criminal activities that score lower than the associated average at the county, state, or national levels. This is a clear indication that the facility, its personnel, and its physical assets are at risk from malevolent actors.

While crime is currently above average, this activity does appear to be trending down. The CAP category in Riverside County has dropped by over 10 percent since 2010, and it is projected to drop another 6.5 percent in the next five years. Similarly, CAP have dropped 11 percent since 2010, and are projected to hold stable for the next five years (2027). While these trends indicate positive progress, burglary, one of the primary concerns at the RWQCP site, has grown by 6.5 percent since 2010.

Overall, the data indicates that the RWQCP is susceptible to malevolent attackers and needs to take strong and effective measures to address these risks, especially given the potential consequences of a criminal intrusion.

Section 5

FINDINGS

This section presents the findings of the security assessment, based on the methodology presented in Section 3 and the threat profile presented in Section 4. The results are presented for each layer of security, as described in Section 3.3.1, relative to meeting both the ANSI 57-10 Standard guidelines and industry best practices for physical, electronic, and operational security measures.

The following subsections are organized by security layers 1 through 5 to match security best practices. The ANSI 57-10 Standard is used to supplement the best practices analysis, serving as the benchmark for each respective security measure. Security measures are organized into various categories, and sub-categories, as detailed within this section of the study. The following sections provide a more detailed description of the benchmarking metrics, and how they apply to each of the individual security layer recommendation tables.

5.1 Benchmarking Security Measures Table

The ANSI 57-10 benchmarking metric table, Table 5, matches the ANSI Standard text, with some minor additions. Each of the table elements are defined below:

- "ID#" - This column assigns each security measure a unique identification number. These numbers are important, as they are referenced within the specific recommendation tables for each security layer. Each security category within a security layer is comprised of several of these security measures.
- "Security Measure" - This column identifies each ANSI 57-10 defined security measure.
- "System Objective " - This column identifies whether the purpose of a given security measure is to delay or detect an intruder.
- "Vandals, Criminal, Saboteur, Insider" - These columns identify the design basis threat for each security measure, i.e., which type of threat the given security measure applies to, and whether that measure can delay/detect a basic or enhanced level of that threat. Refer to the design basis threat matrix in Table 4 for details on what constitutes each threat.
- "Finding" - This column provides a high-level commentary on the RWQCP security profile through the lens of each security measure. A color legend precedes the benchmarking table and helps define the green, yellow, red, and blue colors used. Note that the yellow cells (partially meets) often indicate a situation where the security measure is fully implemented in some parts of the plant, but not in others. In many cases, the measure may not be required in those other applications.

Table 4 ANSI 57-10 Design Basis Threat Capability Matrix

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

Abbreviations: IEDs - improvised explosive devices; IIDs - ignition interlock devices; SCADA - supervisory control and data acquisition.

Table 5 ANSI 57-10 Standard Benchmark Security Measures

Color Legend:

Fully meets ANSI 57-10 benchmarks and security best practices
Partially meets ANSI 57-10 benchmarks and security best practices
Does not meet ANSI 57-10 benchmarks and security best practices
Measure is not applicable to this facility

ID#	Security Measures	System Objective		Vandal		Criminal		Saboteur		Insider		Finding
		Delay	Detect	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced	
1	Basic perimeter fence	◆		✓								Meets
2	Enhanced climb resistant fence	◆			✓	✓	✓	✓	✓			Partially Meets
3	Prevent tunneling	◆						✓	✓			Does Not Meet
4	Bollards/barriers preventing vehicle access	◆							✓			N/A
5	Perimeter IDS		◆		✓		✓	✓	✓			Does Not Meet
6	Keyed gates	◆		✓		✓		✓		✓		Meets
7	ACS gates	◆	◆		✓		✓		✓		✓	Partially Meets
8	Intercom/remote for visitors	◆	◆		✓		✓		✓		✓	Meets
9	Sally port for delivery	◆	◆				✓	✓	✓			N/A
10	Guardhouse/manned entry	◆	◆						✓			N/A
11	Perimeter lighting		◆	✓	✓	✓	✓	✓	✓			Partially Meets
12	Gate area lighting		◆		✓		✓	✓	✓			Partially Meets
13	Hardened openings	◆		✓	✓	✓	✓	✓	✓			N/A

ID#	Security Measures	System Objective		Vandal		Criminal		Saboteur		Insider		Finding
		Delay	Detect	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced	
14	Visitor sign in checkpoint	◆	◆						✓			Meets
15	Warning signs every 50'			✓	✓	✓	✓	✓	✓			Partially Meets
16	Motion lighting		◆		✓		✓	✓	✓			Does Not Meet
17	Clear zone from perimeter	◆	◆		✓		✓	✓	✓			Partially Meets
18	Parking 30' from key areas	◆							✓			Meets
19	Internal fencing layer	◆						✓			✓	Does Not Meet
20	Enhanced internal fencing	◆							✓			Does Not Meet
21	IDS on internal fence	◆	◆					✓	✓		✓	N/A
22	Tunnel resistant internal fence	◆						✓	✓			N/A
23	Bollards at critical exterior equipment	◆			✓		✓	✓	✓			Partially Meets
24	Vehicle barriers at second fence	◆							✓			N/A
25	ACS on second fence	◆	◆					✓	✓		✓	N/A
26	Exterior transformers with cage or barrier	◆			✓			✓	✓	✓		Partially Meets
27	Generators locked cage or barrier	◆			✓		✓	✓	✓	✓		Meets
28	MCC protected barriers	◆			✓			✓	✓	✓		Meets
29	IDS on chemical storage and feed areas	◆	◆				✓		✓		✓	Does Not Meet
30	CPTED/Landscaping/Obstructions		◆	✓	✓	✓	✓	✓	✓	✓	✓	Partially Meets

ID#	Security Measures	System Objective		Vandal		Criminal		Saboteur		Insider		Finding
		Delay	Detect	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced	
31	Manholes locked with security fastener	◆		✓	✓					✓		Meets
32	IDS on manholes	◆	◆		✓				✓		✓	Does Not Meet
33	Limit signage identifying critical assets	◆		✓	✓			✓	✓			Does Not Meet
34	Locking caps for valve operator covers	◆						✓	✓	✓		Does Not Meet
35	Vault hatches locked with shrouds	◆		✓								Partially Meets
36	Vault hatches double door with shrouds	◆			✓			✓		✓		Does Not Meet
37	Vault hatches locked with shrouds with IDS	◆	◆						✓		✓	Does Not Meet
38	Tamper resistant hinges	◆			✓	✓	✓	✓	✓			Does Not Meet
39	Key locked doors	◆		✓		✓				✓		Meets
40	Exterior doors alarmed		◆		✓		✓	✓	✓	✓	✓	Does Not Meet
41	ACS on doors	◆	◆		✓		✓	✓	✓		✓	Does Not Meet
42	Automatic locking critical doors with ACS	◆	◆				✓	✓	✓	✓	✓	Does Not Meet
43	Lobby mantrap	◆	◆						✓			Partially Meets
44	Visitor waiting area	◆	◆				✓		✓			Meets

ID#	Security Measures	System Objective		Vandal		Criminal		Saboteur		Insider		Finding
		Delay	Detect	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced	
45	Blast resistant doors	◆							✓			Does Not Meet
46	Vehicle barriers protect vehicle door	◆					✓		✓			N/A
47	Break resistant windows	◆		✓	✓	✓	✓	✓				Does Not Meet
48	Blast resistant windows	◆							✓			Does Not Meet
49	GB at windows		◆		✓		✓	✓	✓			Does Not Meet
50	Interior IDS		◆				✓		✓	✓	✓	Does Not Meet
51	Barriers on skylights	◆			✓	✓		✓				N/A
52	IDS on skylights	◆	◆				✓		✓		✓	N/A
53	Locked roof hatches	◆		✓	✓	✓		✓		✓		Meets
54	IDS on roof hatches	◆	◆				✓		✓		✓	Does Not Meet
55	Roof access ladders protected	◆		✓	✓	✓		✓		✓		Partially Meets
56	Roof access ladders with IDS	◆	◆				✓		✓		✓	Does Not Meet
57	Indoor transformer with cage	◆						✓	✓	✓		N/A
58	Indoor generator with cage	◆					✓	✓	✓	✓		N/A
59	Indoor MCC with cage	◆						✓	✓	✓		Partially Meets
60	Chemical fill lines locked	◆			✓	✓		✓	✓	✓		Meets

ID#	Security Measures	System Objective		Vandal		Criminal		Saboteur		Insider		Finding
		Delay	Detect	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced	
61	Chemical fill lines locked with IDS	◆	◆				✓		✓		✓	Does Not Meet
62	Indoor chemical storage and feed locked	◆				✓		✓		✓		Meets
63	Indoor chemical storage and feed locked with IDS	◆	◆				✓		✓		✓	Does Not Meet
Water Quality Monitoring												
64	Online water quality monitoring		◆					✓	✓		✓	Meets
CCTV Alarm Assessment												
65	CCTV assessment - exterior doors		◆		✓		✓	✓	✓	✓	✓	Does Not Meet
66	CCTV assessment - hatches and vaults		◆		✓		✓	✓	✓		✓	Does Not Meet
67	CCTV assessment - main gate		◆					✓	✓	✓	✓	Does Not Meet
68	CCTV assessment - main entrance door		◆					✓	✓	✓	✓	Does Not Meet
69	CCTV assessment - general surveillance		◆				✓	✓	✓	✓	✓	Partially Meets
70	CCTV assessment - interior critical areas		◆					✓	✓	✓	✓	Does Not Meet
Power and Wiring Systems												
71	Electrical panels locked	◆		✓	✓	✓	✓	✓	✓	✓		Partially Meets
72	Backup power to security components	◆	◆		✓		✓	✓	✓	✓	✓	Meets

ID#	Security Measures	System Objective		Vandal		Criminal		Saboteur		Insider		Finding
		Delay	Detect	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced	
73	Wiring in conduit	◆		✓	✓	✓	✓	✓	✓	✓	✓	Meets
74	Redundant wiring paths	◆							✓		✓	Does Not Meet
75	Supervised security wiring	◆			✓		✓	✓	✓	✓	✓	Meets
76	Redundant critical utilities	◆							✓		✓	Meets
SCADA - Physical Security												
77	Locked programmable logic controller/RTU enclosures	◆		✓	✓	✓	✓	✓	✓	✓		Meets
78	Tamper switches on enclosures		◆		✓		✓	✓	✓	✓	✓	Does Not Meet
79	Instrumentation wiring in conduit	◆		✓	✓	✓	✓	✓	✓	✓	✓	Meets

Abbreviations: IDS - intrusion detection system; MCC - motor control center.

5.2 Best Practice Assessment Tables

The following sub-sections are divided into the five different security layers, as detailed previously. A best practice assessment table is included for each layer, aligning closely to the metrics identified in the ANSI 57-10 Standard benchmarking table. Each best practice assessment table includes the following:

- An overview of the applicable security best practices.
- A discussion of the existing conditions at the RWQCP.
- A reference to the ANSI 57-10 security measure that aligns with the given security layer category.
- Recommendations to address the vulnerabilities.
- Implementation priority.

Adhering to best practices is essential for effective and defensible security decision making and ensuring future site improvements contribute to a safer and more secure working environment. Specific best practices are shown in italics with supporting information shown in non-italics. Note that best practices are not specifications, i.e., they are not intended to provide specifics regarding design and installation. The intent of these practices is to ensure consistency in the application of mitigation measures across the organization.

5.3 Layer 1 - Site Perimeter Security

Layer 1 security comprises the outer site perimeter of the plant, including fencing and gates on the perimeter, devices to prevent vehicle forced access, and vegetation or structures on or adjacent to the perimeter that may provide or prevent access. Layer 1 also includes the various security technologies deployed on the plant perimeter. These measures are the first line of defense, and security controls implemented here can serve multiple functions, including deterrence, delay, and detection.

Table 6 includes a detailed discussion of the Layer 1 security measures, including existing RWQCP conditions, a comparison to security best practices and the ANSI 57-10 guidelines, and recommendations to reduce risk. Site visit photographs are provided in Appendix B.

Table 6 Layer 1 - Site Perimeter: Security Findings and Recommendations

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Layer 1 - Physical					
Perimeter Fencing	• All perimeter fences and walls should be a minimum of eight feet in height (from the insecure side). Chain link fence should be equipped with three strands of barbed wire on top. Non chain link fence should be equipped with an anti-climb system. Where acceptable by local practices, razor wire is superior to and should be used in lieu of barbed wire. Other detection and assessment tools should be used in conjunction with perimeter barriers, as appropriate for the level of risk. • A barrier is often used as the first line of defense in protecting a facility, and thus, is a critical element of the initial security layer. Chain-link fence is the most common of these barriers due to its durability and relatively low cost. However, the use of fencing or walls is, at best, a deterrent to casual intruders and a short delay to serious intruders. A fence or wall alone should in no way be considered an effective security mechanism. A determined intruder will easily circumvent most fence barriers, chain-link or otherwise. The use of detection and assessment tools, such as fence alarming and CCTV, enhances the barrier function to provide a useful security countermeasure. Any building having public access that also makes up part of the perimeter requires additional attention/hardening. • Access through the perimeter does not always occur at a fence or gate. At a wastewater plant, access is often possible via a water channel or culvert that runs under the fence. Where such conditions exist, the culvert or channel must be blocked or otherwise protected from unauthorized entry.	• Perimeter fencing at the RWQCP is one of the strongest existing security elements. • A majority of the plant is surrounded by wrought iron Impasse II fencing that is at least 8-feet high on the insecure side. This fencing is new and in excellent condition. • Fencing near the septic drop off area in the northeast portion of the plant does not meet the standard. It is a chain-link fence approximately 6-feet tall. There is barbed wire and, in some cases, razor wire topper on this fence. The fence is not grounded and can be easily pulled up to allow access underneath. • The west perimeter includes area equipped with an interior chain-link fence, creating a secondary barrier. This fence was installed prior to the current wrought iron fence installation and can be easily circumvented once inside the main perimeter, providing no real value. There are several areas of disrepair in this fence and it is not necessary for site security. • An area on the west site perimeter has evidence of erosion or individuals penetrating under the Impasse fence. It represents a security concern wherever the ground can be eroded away or easily tunneled. • There are no culverts or other access points to the site.	• **ID#1** - The Impasse fencing provides an effective delay mechanism against potential intruders. The chain link fence in the northeast plant area does not meet best practices. As indicated in the best practices discussion, fencing alone will not prevent incursions. • **ID#2** - The wrought iron fence meets the definition of an enhanced climb resistant fence. The chain link fence to the east does not. • **ID#3** - The existing fencing does not prevent tunneling. The perceived threat at this plant does not justify the cost of installing a 12-24" concrete base/footer for the fence at this time. However, installing the footer in selected areas susceptible to erosion may be beneficial. • **ID#4** - There are no bollards preventing vehicle access around the perimeter. This is not perceived to be an issue as the threat review does not indicate a need for bollards around the entire perimeter. • **ID#13** - There are no culverts that require protection. • **ID#19 to 22, 24, 25** - There is no requirement for internal fencing at this facility.	• **R1** - Improve fencing in the northeast area of the plant. The improvements would ideally be consistent with the Impasse fencing installed throughout the remainder of the site. However an improved chain link installation, along with appropriate intrusion detection measures, would also be effective and less costly. • **R2** - Provide a concrete barrier under the fence in areas where erosion is allowing entry underneath.	• **R1** - Medium priority. • **R2** - High priority.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Gates	• Wherever possible, sliding gates should be used in lieu of swing gates. The crash rating of gates should be based on a detailed threat assessment. The gate area should include a turnaround for vehicles that prevents entry into controlled areas. • Gates are a critical element of the perimeter, and typically a weak point for entry. One of the major issues with gates is the strength of the gate when hit by a vehicle. Swing gates that join in the middle of the road provide minimal protection from this type of attack. The center point where the gates meet is the weakest area, and a vehicle attacking this point can easily breach the gate. The use of a sliding or rolling gate mitigates this weak point, establishing the quality of the gate material itself as the major factor in its ability to withstand an attack. • At many industrial facilities, it is not unusual for large trucks to deliver materials (i.e. chemicals, sludge hauling, etc.). On occasion, these trucks may be directed to the wrong facility, or are denied entry for various reasons. It is important that the gate area provides the ability for these trucks to turn around without having to enter the site. Securing the perimeter and then allowing unauthorized persons and vehicles on-site, intentionally, would compromise security efforts.	• The main gate at RWQCP meets best practices. The gate is a wrought iron powered sliding gate that is a minimum of eight feet in height. The controls for the gate are located inside the secure area. The gate is equipped with ACS, CCTV, and an intercom, and can be remotely operated by administrative or operational personnel within the plant. • Other gates around the perimeter are manual and match the wrought iron fencing. The gates are padlocked and never left open. They are not equipped with intrusion detection devices, and CCTV is limited for some gates. • There is currently no gate that separates the septic drop off area from the main plant. Although access to that area is controlled at the main entry, there is no way to stop someone from moving from this area to the process areas.	• ID#6 -Gates are either access controlled or properly keyed. • ID#8 - The main gate and the septic drop off area gate include Airphone intercoms, which connect to the main reception area. The gates can be opened remotely once contact is made. • ID#9 - The gate areas do not include sally ports (i.e., no protected points of entry into a secure location). This represents a large potential expense that would not notably enhance security against perceived threats. • ID#10 - There is no guardhouse at the main gate. This represents a large expense that would not notably enhance security against perceived threats. • ID#12 - The main gate area and the north gate (near the stormwater pond) are well lit. Other gated areas, which are rarely used, are not typically well lit. Refer to Appendix A for more detail.	• **R3 -** Add fencing and a gate to prevent the ability to move from a public area (septic drop off) to a controlled area (plant process areas).	• **R3** - High priority.
CPTED	• CPTED principles should be consistently applied to all security design, including: – Natural Surveillance - keeping areas well lit, eliminating hiding spots, removing obscuring vegetation, using CCTV where no natural sight lines exist. – Natural Access Control - reducing straight-line access routes using barriers, curbs, and landscaping to direct vehicles. – Territorial Reinforcement - creating a sense of ownership by clearly identifying public/controlled/restricted zones using signs, barriers, access control, visitor/employee badging, and lighting. – Maintenance - ensuring areas are well maintained, indicating constant presence and vigilance.	• There is some level of perimeter lighting at the site. The main gate area is well lit, as is the north perimeter, which includes new lights inside of the fence line. Refer to Appendix A for recommendations associated with additional lighting. • There are areas along the perimeter, notably the south side and near the southwest gate, where vegetation and other material facilitates access to the site. In the southwest corner of the site, just beyond the fence, but well hidden in the trees, there is someone living in a tent. Under the current conditions, that individual would be able to easily enter the site undetected.	• ID#11 - Lighting along the perimeter in areas where personnel travel at night is sufficient. However, current conditions are not appropriate for security. Other technologies (thermal, infra-red) can preclude the need for visible lighting in most cases.	• **R4** - Clear all vegetation from the fence line, creating a clear zone that inhibits both access and hiding places. • **R5** - Work with neighboring businesses to limit the amount of material stacked against the fence line.	• **R4/R5** - Low to medium priority.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Signs	• *Signs should be used to enforce the CPTED concept of territoriality. Ideally, signs should be placed at 50-foot intervals around the perimeter.* • The concept of territoriality involves the use of indicators to establish ownership or control. These types of indicators perform two functions: – Warn off casual criminals. – Provide a psychological notice that "you are being watched". • Signs should not provide excessive information to intruders, but must provide necessary information to first responders.	• There are ample signs at the main gate area. Signage is not in place every 50-feet on the perimeter, but rather at areas near gates and entrance points.	• ID#15 - Signage does not meet the standard of every 50-feet. However, the problems that the RWQCP is facing would likely not be alleviated by more signs. It is readily apparent that this is a private, secure facility. If the fencing is not preventing intruders, signs likely will not either. However, the issue of liability may be relevant to additional signage - is the organization doing enough to prevent a potential lawsuit if someone were to enter the site and injure themselves? • ID#33 - Building signs indicate associated processes. See Layer 3 - Buildings for recommendations.	• **R6** - Discuss liability concerns with internal City risk group to determine if additional signage is warranted.	• **R6** - Low priority.
Lighting	• Lighting should be utilized to accomplish multiple goals. – Support the CPTED concept of territoriality. – Create a deterrent to potential intruders. – Provide a level of comfort for staff. – Complement CCTV systems, as necessary.	• Refer to Appendix A for more detail. There is currently no Layer 1 motion lighting installed to complement CCTV systems. The use of thermal or other technologies would preclude the need for visible light.	• ID#16 - Although the site is currently not meeting the ANSI 57-10 guidelines, the use of other technologies can provide the security benefits that drive installation of motion lighting. While motion lighting to deter, detect, and assist CCTV surveillance is useful, it is often flawed, as lights can fail or not activate in time to achieve their purpose.	• To support plant operations and staff safety, new lighting should be installed at the west perimeter (HM-7, HM-8, and HM-9). To support facility security, new lighting should also be installed at the Storage Area (HM-11). Refer to Appendix A for more detail.	• N/A.
Layer 1 - Electronic					
Intrusion Detection	• The entirety of the perimeter at an industrial facility should be alarmed. The intent of the alarming is to identify when a breach of the perimeter occurs. Where possible, alarming should include a corridor exterior to the facility perimeter itself to identify potential breaches. • Effective perimeter alarming can be achieved using various technologies. These include on fence cable systems, ground buried sensors, volumetric (microwave) beams, optical beams, and intelligent video alarming. Each method has its own benefits and challenges, and the correct technology will depend on many local factors, including cost.	• Layer 1 of the RWQCP currently has no perimeter IDS. There are cameras that can be used for this purpose, but they do not cover the entire perimeter. The City is currently testing several mobile cameras on the north perimeter to determine feasibility. • The site is equipped with numerous cameras, connected to a Genetec VMS (a high-end video platform). The Genetec VMS, and associated cameras, are capable of providing significant security utility, in addition to their current process functions.	• ID#5 - There is no perimeter IDS.	• **R7** - Install a CCTV system to provide perimeter protection, utilizing a combination of thermal and pan-tilt-zoom (PTZ) cameras. The thermal cameras would primarily be located along the perimeter, although in some areas they could be placed on buildings. The PTZ cameras would be tasked to the thermal cameras and provide secondary alarming and alarm assessment. The existing Genetec system is capable of the above performance integration. Implementation can be phased - ensuring the appropriate platforms are specified - adding devices as time and budgets allow. The priority is the north fence line, which has experienced the most issues to date. As an interim measure until the City can design and implement the recommended permanent CCTV system solution, the City should continue to employ (and potentially expand the use of) the ECAMSECURE mobile units to meet the immediate security needs of the RWQCP. Refer to the CCTV Evaluation Tech Memo provided in Appendix C.	• **R7** - High priority - add intrusion detection to the north fence line. • **R7** - High priority - utilize existing equipment to provide alarming at main gate. • **R7** - Medium priority - add intrusion detection to the remaining perimeter.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Alarm Assessment	• Alarms on the perimeter require monitoring personnel or systems to evaluate the alarm and determine appropriate response. • Understanding the causes of an alarm will support appropriate response. It is critical that personnel tasked with alarm response have as much accurate information available to them as possible. This is both a safety and a security concern.	• There are currently no alarms within Layer 1 (i.e., there is no assessment capability). The plant control room is staffed and could provide necessary assessment capabilities (given the correct tools). In addition, as some of the CCTV is currently monitored by the City off site, there is an expectation that assessment could occur there. Refer to Section 5.4 for additional discussion on system monitoring.	• **ID#65 through 70** -There is currently no consistent alarming or monitoring on site, and therefore no assessment of alarm conditions.	• **R8** - Ensure that, as alarms are added to the perimeter (See: Layer 1 - Intrusion Detection), complementary assessment capabilities are provided to assess these alarms. Assessments can be performed on site by RWQCP staff, off site by the City, or remotely (iPad, laptop) through a process which sends alarms to on call RWQCP personnel. Refer to Section 5.4 for additional recommendations related to system monitoring.	• **R8** - High priority.

5.3.1 Layer 1 – Interim CCTV Solution

As part of this effort, a separate CCTV Evaluation was completed to help the City determine the value of extending the rental period of their ECAMSECURE mobile CCTV units, pending a permanent CCTV/perimeter security solution at the RWQCP. The technical memorandum (TM) is included in Appendix C.

The primary finding of the CCTV evaluation was that the optimum long-term solution includes the provision of appropriate perimeter security at the RWQCP, which will include installation of permanent technology to guard the fence line and other critical areas of the facility. However, as an interim measure until the City can design and implement the recommended permanent solution, the City should continue to employ (and potentially expand the use of) the ECAMSECURE mobile units to meet the immediate security needs of the RWQCP. The units should be equipped with thermal devices, which will provide a more efficient and cost-effective way to combat intrusions along the perimeter (versus visible light cameras). Depending on available budget, the installation can be phased to address the most problematic areas of the perimeter first. See Appendix C for additional details.

5.4 Layer 2 - Clear Zone Security

Layer 2 security comprises the clear zone of the plant, i.e., the area between the perimeter and any internal structures. Generally, this area is more difficult to surveille and alarm, as there are often very wide areas of unused space. Use of CCTV and CPTED techniques are often the most effective controls for this Layer. Layer 2 security controls are used primarily as detection factors.

Table 7 includes a detailed discussion of the Layer 2 security measures, including existing RWQCP conditions, a comparison to security best practices and the ANSI 57-10 guidelines, and recommendations to reduce risk. Site visit photographs are provided in Appendix B.

Table 7 Layer 2 - Clear Zone: Security Findings and Recommendations

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Layer 2 - Physical					
CPTED	• CPTED principles should be consistently applied to all security design including: – Natural Surveillance - keeping areas well lit, eliminating hiding spots, removing obscuring vegetation, and using CCTV where no natural sight lines exist. – Natural Access Control - reducing straight-line access routes using barriers, curbs, and landscaping to direct vehicles. – Territorial Reinforcement - creating a sense of ownership by clearly identifying public/controlled/restricted zones using signs, barriers, access control, visitor/employee badging, and lighting. – Maintenance - ensuring that areas are well maintained, indicating constant presence and vigilance.	• There are several areas along the plant perimeter that provide site access and hiding places for intruders. Most notable are portions of the south fence line. In addition, an adjacent business on the south side has scaffolding along the perimeter that rises above the RWQCP fence and provides a platform for illegal entry. • Inside the plant perimeter, natural surveillance requirements are met. Maintenance is mostly effective, and the site does not invite intrusions due to lack of care. • CPTED identifies value in locating parking areas away from key process areas. This guideline is met, as the main parking area is separate from any process. However, this does not preclude a vehicle from moving around the site. • Each building has a sign noting its function. This provides knowledgeable intruders with a road map of where to go to cause the most damage.	• ID#17 - Other than the items noted within the Layer 1 recommendations, the plant clear zone meets standard requirements. • ID#18 - Parking areas are separated from process buildings. • ID#30 - There are no major obstructions created by landscaping within the plant. • ID#33 - Plant buildings all have signs indicating which process is inside.	• **R9** - Remove vegetation, as indicated in R4. Work with neighboring businesses to reduce the opportunity for access on the south fence. • **R10** - Over time, replace signs on buildings with a numbering system known to staff only. In an emergency, responders can be directed to "Building 4" rather than "Headworks".	• **R9** - Medium priority. • **R10** - Low priority.
Equipment	• Exposed critical process equipment should be protected by bollards or other barriers. These bollards are intended to provide protection against malevolent actors and vehicles legitimately on site. • External equipment, such as exposed cabinets, manholes, and generators should be properly secured and protected using physical (locks, bollards, fencing) and electronic (IDS) means. • The level of recommended equipment protection is dependent on the value of the equipment and the perceived risk to it. Manholes can be secured using a security bolt requiring a specific tool. Ladders to tank roofs can be effectively secured using physical barriers and locks. All external equipment should be under surveillance in a properly designed environment, presenting opportunities for effective intrusion detection.	• Existing generators are located outdoors and protected by bollards. They are key locked and, in some cases, can be viewed with existing video devices. However, the generators are not alarmed. MCC equipment is located inside buildings that are typically locked via key only. There are cabinets or small lockers housing equipment that are not well secured. • Access to tank ladders are secured with a cap and lock. In some cases, these locks are ineffective as the cap has been pulled aside. • Manholes at the site are secured. Manholes are not equipped with IDS.	• ID#23, 26 - Bollards are installed in multiple areas (generators, other). However some transformers are not protected with either cage or bollard. • ID#27 - Generators are well protected. • ID#28 - MCC equipment is protected, inside buildings. • ID#31 - Manholes are locked with a security tool. • ID#32 - Manholes are not equipped with IDS. Given the threat environment, this approach would not provide enough benefit to warrant the cost.	• **R11** - Review key electrical equipment locations (exterior) and add bollards as necessary. – Most equipment is well protected and there is minimal traffic near the exposed equipment. Bollards in this case are intended to prevent an accident more than to prevent an attack.	• **R11** - Low priority.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Intrusion Detection	• Layer 2 areas should provide maximum opportunity to detect trespassers. Routes to and from critical assets through the clear zone should be surveyed where possible. • In many facility attacks, the clear zone is where an intruder will be visible for the longest period. Additional assessment can occur within this zone after a perimeter breach. Typically, video surveillance is the most appropriate way to generate alarms in this layer. • An internal perimeter fence with intrusion detection is generally used in very high security environments.	• No IDS exists within the plant's clear zone. This includes chemical storage and feed areas, although those areas can be viewed by CCTV to some extent. Effective implementation of CCTV throughout the site will allow all key areas to be properly alarmed. These areas can be identified either directly or as part of a prioritization workshop.	• ID#25 -There is no secondary fence requiring alarms, nor is there a need for one. • ID#29 - There is no IDS for the chemical feed and storage area. • ID#32 - There is no IDS on manholes.	• **R12** - Develop a video design strategy that leverages existing platforms and equipment and provides a comprehensive video surveillance and alarming approach for the entire site. This includes the perimeter, clear zone, and internal alarming. • There are numerous cameras throughout the plant and an excellent video platform in place (Genetec) that can be leveraged to provide the necessary alarming.	• **R12** - High priority.
Alarm Assessment	• Alarms in this layer require a methodology to allow monitoring personnel or systems to evaluate the alarm and determine appropriate response. • Understanding the causes of an alarm will support appropriate response. It is critical that personnel tasked with alarm response have as much accurate information available to them as possible. This is both a safety and a security concern.	• The plant has no alarms in Layer 2. Appropriate use of video would address this gap.	• ID#59 - Some existing cameras currently view Layer 2 areas and could be used to support alarming and alarm assessment.	• **R13** - As alarming capability is added to Layer 2 via video or other means, provide assessment capability as described in Layer 1 - Alarm Assessment. – Alarming and alarm assessment using existing and future video capabilities should be a very high priority moving forward.	• **R13** - High priority.

5.5 Layer 3 - Building Security

Layer 3 security comprises the security controls deployed at the envelope of the building and represents controls that are both physical (strong doors and locks, protected windows) and electronic (access control, CCTV, intrusion detection). These controls are not associated solely with doors and windows, but also the roof, attached vaults, and any other portion of the building that could provide access. Layer 3 controls also serve multiple functions (deterrence, delay, detection) and in many cases can help determine an appropriate response methodology.

Table 8 provides a detailed discussion of Layer 3 security measures, including existing RWQCP conditions, a comparison to security best practices and the ANSI 57-10 guidelines, and recommendations to reduce risk. Site visit photographs are provided in Appendix B.

Table 8 Layer 3 - Buildings: Security Findings and Recommendations

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Layer 3 - Physical					
Doors/Locks/Hinges	• Exterior doors for buildings holding critical assets should have the following: – Mechanical locks with Medeco IC or similar removeable core for doors without access control. – Hinges to buildings housing critical assets should be security hinges requiring a special tool to remove, should be located on the secure side of the door, and should be tamper resistant.	• All plant doors are equipped with lock and key. • There is no intrusion detection in place for perimeter doors. • Process building doors are metal in metal frames and secure. • There are a variety of astragals used across the site, from a full astragal to a smaller astragal covering only the lock set. • Hinges are typically installed on the outside of doors and are not purposefully tamper resistant. • Doors are not blast resistant.	• **ID#38** - Hinges are not tamper resistant. • **ID#39** - All process area doors are properly keyed. Some are left open for operations in the daytime.	• **R14** - Provide security hinges for all doors. – There is only marginal risk reduction associated with this effort.	• **R14** - Low priority.
Windows/Openings	• Any vent larger than 96 sq. in. must be secured by a grill. The grill should have no less than a 2" screen, and 0.192" diameter wire. 16.5 mm anti-penetration film should be provided where there is a threat of a projectile. Window coverings or blinds should be installed on ground floors or roof access floors. • Where a building could be attacked with a vehicle, appropriate physical measures should be in place, such as bollards, planters, or other barrier material. • Access points to roofs (usually a ladder or stairs) should be secured from unauthorized access.	• Most of the process buildings do not have windows. The Admin/Lab building windows are not protected in any way (i.e. with glassbreak detection, film, or other shatterproof material). The Maintenance Building has accessible windows that are not protected. The remaining process buildings rarely have glass or unprotected openings. • There is no apparent requirement for barriers in front of buildings. The guideline for this element is to protect against an elevated (well equipped, well-armed) saboteur. Such an attacker would have multiple options beyond crashing a vehicle into a building. • Ladders are equipped with cages to prevent access. However, some are not locked or have been damaged. • There are no glass skylights in any buildings that require physical protection.	• **ID#46** - Protection from vehicle attack is not necessary. • **ID#47, 48, 49** - Windows and openings are not well protected. • **ID#51** - There are no skylights. • **ID#53** - Roof hatches are locked. • **ID#55** - Ladders have cages to prevent access. However, some are not locked or have been damaged.	• **R15** - Add glassbreaks. – This is the most cost-effective approach to address this gap. Adding window bars is not warranted given the threat environment and past incident history. • **R16** - Repair the ladders that currently do not inhibit unauthorized access.	• **R15** - Medium priority. • **R16** - Medium priority.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Exterior Equipment	• All exterior critical equipment should be protected. Protection can be physical (locks, chains, etc.) or electronic (CCTV, IDS). However, a combination of both is ideal. • At an industrial facility, critical areas include anything vital to process, as well as areas where dangerous materials are stored.	• Ground vaults and hatches are locked in all cases. Shrouds covering the locks were typically not present, except in rare cases.	• **ID#34** - There are no locks on valve caps. • **ID#35** - While hatches are locked, there are no shrouds protecting the lock. • **ID#36** - Vault hatches with double doors are not shrouded. • **ID#57** - There are no indoor transformers requiring cages. • **ID#58** - There are no indoor generators requiring cages. • **ID#59** - Indoor MCCs are not caged, but they are protected by the building itself. These buildings are well built and not easily susceptible to attack. As this requirement speaks to an elevated type of attack, adding cages is not a high priority given the other necessary security improvements. • **ID#60** - Chemical fill lines are locked. • **ID#62** - Indoor chemical storage areas are secured.	• N/A. – ID#34 and #36 are intended to delay a saboteur or a well-prepared and equipped vandal. These security measures would provide some delay, but other noted security deficiencies, most notably the inability to deter or detect entry to the site, are far more critical. The fact that these equipment areas are locked meets the primary intent of the guideline.	• N/A.
Separation	• Buildings should be divided into security zones, typically public, controlled, or restricted. Each zone should be secured by lockable doors, including access control. Zone separation areas should be in view of CCTV. • Public areas do not imply the public has full access to these areas - in an industrial facility the public area would represent any areas where visitors or contractors first interface with reception or other personnel. Controlled areas should require escort for any non-employee and should be separated for employees based on job requirements. Restricted areas are those which only a person with specific credentials would be able to access, e.g., control rooms, electrical rooms, communications closets, and server rooms.	• Most of the process buildings have only one room. Generally, if an individual is permitted to access one part of the process area, they are likely permitted in remainder of that building. • The Admin Building contains multiple rooms, including a waiting area for visitors separated by glass doors (although these doors are typically open during the day). There is no security within the building that would inhibit an intruder from moving to controlled or restricted spaces. • The Server Room and the Control Room are not controlled or protected in any manner. These should be considered high security areas that merit additional security.	• **ID#43** - The lobby area could be used as a mantrap with the application of ACS. It is not appropriately secured at this time. • **ID#44** - See above. The visitor waiting area and lobby can be used effectively to meet this guideline with the application of technology.	• **R17** - Create separation within the Admin Building by adding ACS to the doors separating the common area from the interior. • **R18** - Add ACS to the server room door. Add ACS to the Control Room door.	• **R17** - Medium priority. • **R18** - High priority.
Access Controls	• Each building should have at minimum of one entry door equipped with automated access control (card reader, alarm contact, request to exit, door position switch). Where possible, all perimeter doors should be part of the ACS.	• Currently, there is very limited use of ACS on site. Only the Admin/Lab Building is equipped with card readers, connected to a Honeywell control panel.	• **ID#41** - Most doors, including critical areas such as the Server Room and the Control Room, are not equipped with ACS. • **ID#42** - There is no auto locking of doors.	• Refer to Table 9 for sitewide access control recommendations. – Implement at critical areas first to prioritize the addition of access control.	• Refer to Table 9 for sitewide access control priorities.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
CCTV	• Cameras should be available to view all entry/exit points from buildings. Use of PTZ cameras integrated with the ACS is preferable (assuming the existence of an ACS).	• There are 33 existing cameras in use at the plant, connected to a Genetec VMS. A majority of the cameras are Avigilon. Both Avigilon and Genetec are high end systems with significant capabilities. However, they are not currently programmed to provide alarming information and assessment to local staff. Essentially, they are view only, controlled elsewhere by the City. To meet or exceed the guideline recommendation for assessment and alarming, the existing cameras would need to be re-tasked to add that function (in addition to their current process functions). Additional cameras would also be required.	• References ID#65-70 are generally relevant to this item and are addressed in the sitewide CCTV section below (Table 9).	• Refer to Table 9 for sitewide CCTV recommendations.	• Refer to Table 9 for sitewide CCTV priorities.
Intrusion Detection	• All perimeter entry points (doors, overhead doors, roof hatches, windows) should be equipped with IDS. The IDS requirement can be met using video, alarm contacts, passive infra-red detectors, glassbreaks, or other technologies.	• There is no intrusion detection currently in place at the facility.	• **ID#37, 40, 41, 42, 49, 50, 54, 56** - There are no intrusion detection devices on building doors, windows, or internal areas. • **ID#52** - There are no skylights requiring IDS. • **ID#63** - There is no IDS associated with chemical storage areas.	• **R19** - Add IDS to building perimeter entry/exit points. This can be accomplished via actual intrusion contacts, or the expanded use of video. Include any roof hatches in this effort.	• **R19** - Medium priority.
Internal Alarms	• Key areas within any building should be equipped with intrusion alarming. Key assets within that building should be equipped with video surveillance and alarming. • Key areas include assets critical to the mission of the organization, as well as the separation areas noted above between public/controlled/restricted spaces. Alarms can be driven by several technologies, including video, alarm contacts, passive infra-red detection, and acoustic sensors. The technology selected should reflect specific area needs and capabilities.	• None of the buildings currently include internal alarms or video surveillance.	• **ID#49, 50, 52, 54, 56** - Refer to Table 9 for sitewide intrusion detection references	• Refer to Table 9 for sitewide intrusion detection recommendations.	• Refer to Table 9 for sitewide intrusion detection priorities.

5.6 Layer 4 - Sitewide Security

Layer 4 security comprises sitewide security measures and includes tools applicable to all security layers within the RWQCP facility. For example, while the placement of cameras is relevant to the first three layers, it would be redundant to discuss the use of CCTV platforms for assessment and monitoring at each layer. Instead, this discussion is included as part of Layer 4.

As noted in Section 3.2.2, guard services can also provide a visible deterrent to help prevent criminal activity, as well as the ability to quickly respond to any intrusions. However, such a service can be extremely costly – especially at a large site like the RWQCP.

The next best option is an effective perimeter protection system, integrated with an effective interior protection system, with detailed monitoring and response protocols based on the information that is provided by these systems (as recommended in the other layers). While the capital costs for this approach can be higher, the level of security provided is extensive and annual operating costs are far less than associated with a full-time guard service. Consequently, while a guard service may provide interim value until the recommended systems are implemented, it is not considered a long-term solution for the facility.

As described in Section 5.3.2, implementing a mobile CCTV solution is another interim measure that can provide value until a long-term perimeter security system is in place. In comparing the use of a guard service to the use of mobile CCTV units as an interim security solution, the mobile CCTV units are the recommended solution. While a combination of both guard services and CCTV is the most effective security approach, there is a substantial cost to having both guards and CCTV coverage. The best compromise is to install a CCTV system with thermal imaging, as it can provide an effective means to providing wide site coverage and creating intrusion detection alarms without the need for physical site presence. Additionally, the site's current guard service has had limited success due to high on-going costs and limited site coverage.

Table 9 provides a detailed discussion of the Layer 4 security measures, including existing RWQCP conditions, a comparison to security best practices and the ANSI 57-10 guidelines, and recommendations to reduce risk. Site visit photographs are provided in Appendix B.

Table 9 Layer 4 - Site Wide: Security Findings and Recommendations

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
System Monitoring	• Adequately trained personnel should monitor security systems around the clock. Ideally, system monitoring should be performed simultaneously on-site and off-site by either organization personnel or contracted personnel at an off-site location designated for security operations. • Effective monitoring of the security system is one of the most critical elements of the entire security plan. Without an effective monitoring component, the entire system can easily be compromised and thus rendered useless. Unmonitored alarms lead to a lack of response, which in turn leads to a lack of system confidence. Sporadic or complete lack of monitoring can lead to an event being discovered after it is too late to intervene or limit damage. • A security system loses an appreciable level of capability if it is not monitored correctly. Real-time monitoring of the system provides an organization with the ability to detect an intrusion, assess it promptly and properly, and respond to it in an appropriate and immediate fashion. In a real-time monitoring approach, monitoring personnel are advised of a breach in the security profile, use tools to assess the breach, and then send contract security or other appropriate personnel to respond. If the assessment indicates a false or nuisance alarm, it can be ignored. • Monitoring should also be undertaken for investigative purposes. The ACS provides a wealth of information that should be utilized to its full extent. As an example, the system pinpoints occasions when a cardholder uses an access card to attempt to access a restricted area. If this event occurs one time it could be happenstance, but if the event occurs multiple times it could indicate a serious problem. Only with proper monitoring and auditing of the system can a pattern of inappropriate card usage be detected. • At larger, manned sites, simultaneous monitoring by on-site and off-site personnel should be considered to provide redundancy. There are distinct advantages of both on-site and off-site monitoring that, when combined, provide maximum security benefits. Both on-site and off-site monitoring stations should be capable of monitoring all security system components. Personnel that are tasked with security functions are far more alert, efficient, and productive when using a fully equipped monitoring station. Monitoring personnel should have a console dedicated to security monitoring and should not have other duties that preclude effective and constant vigilance (i.e., wastewater treatment operation).	• System monitoring is currently one of the most critical security issues that the City should address. While there are over 30 cameras on site, they are not locally controlled or monitored for alarms. The devices and platforms in place for video are capable of alarming, alarm assessment, surveillance, and investigation - the key functions of any effective video system. Unless the current approach to system monitoring is modified, the systems in place and those recommended in this document will not provide full security value. • System monitoring is not restricted to video monitoring. While there are currently no intrusion devices on site and very little access control, these systems, once implemented, will require monitoring as well. The recommendations herein address methods to do so effectively and within the resource capabilities of the City.	• **ID#65-70** - As noted, there is currently no consistent alarming or monitoring on site, and therefore no assessment of alarm conditions.	• **R20** - Provide exception-based monitoring for all security systems, existing and future. Exception based monitoring includes business rules regarding which events or alarms merit assessment and response. This enables operators to only scrutinize video or other system feeds if a problem has been detected and requires human intervention to solve. This is a core technology that facilitates greater efficiency and reliability in how Control Rooms or Security Operations Centers work. When an event occurs, programming allows the event to pop up on a previously unused black screen, drawing attention to the alarm either visually or audibly. At this point, the operator recognizes that an undesired event (alarm) has occurred, and an assessment and response protocol must be invoked.	• **R20** - High priority.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Alarm Assessment	• Tools should be provided to allow all alarms to be properly assessed. Alarms to be assessed are those created by the access system, intrusion system, and the video system. In industrial plants, alarms can also be generated from process alarms via SCADA. • Without proper assessment, no coherent response can be generated. Safety of responding personnel is also a critical component of the assessment capability. Most often, effective assessment is provided using CCTV.	• Alarm assessment is limited to SCADA alarms, which are not part of this security evaluation. There are no other alarms being generated at the plant. Existing video systems are capable of alarming. • There is currently no IDS and limited access control in place. • At the time of this study, the City was testing three mobile cameras as part of a temporary demonstration project. These cameras, placed at key points along the perimeter, are monitored off site by a third party. Events occurring within the field of view of these units are reported to the RWQCP for response.	• **ID#65 through 70** - See the System Monitoring section of this table (above).	• See System Monitoring Recommendations above. CCTV is the most useful assessment tool available. Once any system begins alarming, CCTV should be utilized to assess the alarm to determine an appropriate response. As security systems are further developed at the site, integration of systems will allow an automated alarm assessment capability.	• See priority above regarding monitoring.
Alarm Response	• All alarms should be responded to. • Response is based on the assessment of the alarm. Operational personnel should not typically be responding to alarms if the alarm has not been assessed. Police or third-party contractors should be tasked with response to verified alarms. On-site staff should not be tasked with alarm response without effective and reliable alarm assessment in place.	• SCADA alarms are addressed by plant personnel. • There are no security alarms in place to require response.	• Alarm response is not noted in the guidelines.	• **R21** - Alarm response protocols must be developed as part of the Operational Security component of the security program. – Most necessary equipment is currently in place to facilitate response. The City should develop protocols via a paper and workshop exercise.	• **R21** - High priority.
ACS Platform	• The ACS is often the managing component of the entire security system. All perimeter access points should be equipped with a card access system to control entry and egress. Each building or structure, including high priority areas within buildings, should be equipped with card access at one entry point (at a minimum). Other perimeter doors should be alarm/exit only if no access is intended at the location. High priority assets should be protected with an ACS requiring a card and an additional verification measure, such as a personal identification number or biometrics. • A threat assessment and asset prioritization process will help identify the buildings and areas within a building that require access control. • An ACS provides a wealth of information that relates to both safety and security. The system should be able to provide reports that can be used as an investigative tool. The following conditions, all of which can be determined via the software, should always be investigated: – Propped doors. – Cards read in unauthorized areas. – Card read at unauthorized times. – Compliance with entry/exit procedures at gates. • Compliance with entry/exit procedures relates to personnel properly carding into the site. For example, when carpooling, often only the driver will read their card to gain entry. This creates both security and safety issues, as it is difficult to determine who is on site.	• There is limited access control at the RWQCP site. The Admin/Lab building is equipped with card reader entry. The main gate and the alternative entry (via the septic area) are also equipped with card readers. The readers are operating on a Honeywell platform. • The main gate area also includes exit readers, which are currently not used. Exit is provided via a ground loop. This approach, while common, creates a vulnerability that allows easy and uncontrolled or unauthorized exit for intruders.	• **ID#7** - The main gate has access control, but the other site entries do not. However, the other entry points are not commonly used. The main gate also has exit readers which are not used. • **ID#25** - There is no second fence that requires access control. • **ID#41** - Without widespread use of an ACS, most areas do not have controlled entry. • **ID#42** - Without widespread use of an ACS, most areas do not have automated door locking.	• **R22** - Generate a strategy to provide a full ACS over time. This can be initiated by selecting the platform (or expanding the existing Honeywell platform, which is a viable option) followed by a prioritization of areas to be controlled. Over a period of several years, doors and areas can be added to the system as funds become available. This can be a medium-term project, taking 2-5 years, or a short-term project if funds are available. • **R23 -** Activate and use the exit readers. This can be programmed to function at certain times. For example, during shift change hours, the system could allow exit via ground loop, per the current approach. After hours, the system could be automatically switched to require an exit read.	• **R22/R23** - High priority.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
	• Card access systems provide access via authentication (e.g., an access card) and authorization, where a given card is accepted. Authorization links authenticate individuals to specific buildings or areas to which they are entitled to have access and do so by establishing rules for each controlled access point. The authorization process is managed by the access system administrator and management. • Authenticity can be provided via three factors: – What you have (a card, a key). – What you know (a personal identification number). – Who you are (biometrics). • The more factors required, the better the security. However, there is a need to balance security requirements with operational efficiency. Typically, using an access card as single factor authentication is sufficient security. However, for high priority assets, multiple factor authentications should be used. • Card access should not be used solely to replace keys. The technology should be leveraged in the manner described above. All card access doors must also include alarm contacts, electrified locks, request-to-exits, and door position indicators.				
CCTV and VMS Platform	• CCTV should be used for alarming, assessment, surveillance, and investigation. The entire length of the perimeter, clear zones, and high priority assets should be monitored by video surveillance. A combination of PTZ and fixed cameras should be used to provide the best possible coverage. The system should have a sophisticated digital video management system capable of geographic information system integration, camera control, video distribution, analysis, sensor integration, and alarm notification. • The CCTV component of the security profile should be viewed as a system that is greater than the sum of its parts. It is important not to consider the cameras separate from the digital video management system, nor the reverse. • Video systems can track activity in their field of view with several different technologies and can trigger alarms when an activity occurs. CCTV cameras should also be used to provide assessment when another detection system creates an alarm. Cameras should be capable of filling a general surveillance role and be used for pre-programmed tours of the complex, when not responding to alarms. Finally, the system should provide a high degree of investigative capability. If video footage is required as evidence, stored video should be easy to retrieve and have assurances that it was not tampered with. • A CCTV system should include a combination of PTZ and fixed cameras. PTZ cameras should be used for overview and alarm assessment, while fixed cameras (including visible light, infrared, and thermal) should be responsible for alarm assessment, general surveillance, and, in some cases, alarm detection. Specific selection criteria for cameras should reflect the criticality of the site, and the environmental conditions that might make thermal or infrared cameras more useful.	• There are currently over 30 cameras on site. The cameras are not utilized in a primary security function and are not tasked with alarming or alarm assessment. The existing system is not fully utilized. • Existing cameras are not integrated to other security systems. • Existing cameras are available to view the gate area, but typically not the various building entry and exit points.	• **ID#5** - Perimeter IDS can be accomplished with video. However, no IDS is in place at this time. • **ID#29** - There is no use of video to protect/provide IDS of external equipment. • **ID#32** - There is no use of video to protect/provide IDS and assessment of external equipment. • **ID#65** - There is no use of video to protect/provide IDS and assessment of external building doors. • **ID#66** - There is no use of video to protect/provide IDS and assessment of hatches and vaults. • **ID#67** - There is no use of video to protect/provide IDS and assessment of main gates. • **ID#68** - There is no use of video to protect/provide IDS and assessment of the main door to Admin/Lab Building. • **ID#69** - There is no use of video to provide increased general surveillance capability. • **ID#70** - There is no use of video to protect/provide IDS and assessment of critical internal areas.	• **R24** - Develop a video surveillance protocol that includes: – Video alarming. – Fields of view including all building entry points. – Full perimeter coverage including the use of thermal, fixed, and PTZ cameras, as appropriate. – Internal CCTV for critical areas (e.g., Server Room). – Development of exception-based monitoring. – Full integration to other security systems as they are rolled out. – Alarm assessment protocol. – Alarm response protocol.	• **R24** - High priority.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Intrusion Alarming Platform	• The perimeter should be equipped with an IDS. All entry points into buildings and structures, including windows and roof hatches, as well as high priority areas within buildings, should be monitored using contacts, motion detection, and/or glass break technology. • There are several ways to protect a site perimeter including sensors on fences, sensors in the ground, or optical/microwave beams. CCTV analytics, including the use of thermal imaging systems, are a very viable approach in areas with very long perimeters or difficult weather environments. Perimeter detection using video can be designed to protect the exterior perimeter, interior perimeter, or both. • Intrusion detection is also utilized on and in buildings. For operations buildings, while access control is typically provided on some doors through an integrated IDS, exit only doors should also have an IDS component to identify forced or held open situations. Other rooms within a building should also include IDS depending on the threat assessment. These rooms might include mechanical or electrical rooms, communications closets, and tool storage areas.	• There are no IDS or associated alarms in place at the plant.	• **ID#5** - Perimeter IDS can be accomplished with video. No IDS is in place at this time. • **ID#21** - There is no internal fence that requires support. • **ID#29** - There is no use of video to protect/provide IDS of external equipment. • **ID#32** - There is no use of video to protect/provide IDS and assessment of external equipment. • **ID#37** - There is no use of IDS for assessment of vaults. • **ID#50** - There is no use of IDS to protect assets internal to buildings. • **ID#54** - There is no use of IDS on roof hatches. • **ID#56** - There is no use of IDS on roof ladders. • **ID#61** - There is no use of IDS on chemical fill areas. • **ID#78** - There is no use of IDS (tamper switches) on SCADA equipment enclosures.	• **R25** - Develop and implement an IDS that combines access control doors, video alarming, and specific intrusion devices to protect: – Entry doors to all buildings. – Separation points between public and controlled and controlled and restricted areas. – Areas within each building where critical assets are held or where personnel might require security. These might include Server Rooms, Control Rooms, Reception areas, and electrical rooms. • Note that many intrusion requirements identified in the ANSI 57-10 Standard can be addressed with the use of video, as described above. All access-controlled doors should also inherently include intrusion detection.	• **R25** – High priority.
System Integration	• Electronic security systems should be designed and installed with consideration for the ultimate goals of the system. Security systems should be integrated seamlessly with each other, allowing a simple and effective user understanding and response to critical situations identified by the systems. • Integration is a central tenet of modern security design. Proper integration provides the end user with greatly enhanced security capabilities, leading to a much higher level of comfort for personnel that are protected by the system. In addition, effective integration reduces training costs, limits maintenance costs, enhances the ability to quickly troubleshoot a system, and provides a more effective security response from personnel. • Integration is the interaction and sharing of information, features, and functionality between systems and people to perform a system function effectively and efficiently. Strong integration reduces the amount of interaction required between technology and people, which has two key benefits: (1) freeing up personnel to perform other functions, and (2) reducing possible points of system failure. • Conventional security contracting methods typically result in several systems from different vendors, each supplying different components of the system. While this is often inevitable, it can create extra training, installation, and maintenance costs for the owner. Developing an integrated system platform design is the preferred alternative. The methodology behind an integrated platform is based on the ability to have differing system components functioning as one, and reporting through the same interface to an operator.	• There are no systems in place, i.e., no system integration.	• The guidelines do not address security system integration.	• **R26** – Ensure that the design of all security systems includes/requires integration that supports a coherent communication at a software level between systems, such that an alarm generated in one system will generate an assessment in other systems automatically. • The integrated system should also automatically contact the appropriate personnel via multiple methodologies.	• **R26** - Medium priority. • Integration is accomplished after other recommended systems are implemented.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
	• An integrated platform approach provides several advantages to the user. There is an increase in system functionally and reduction in training costs, as the operator is only required to learn one interface for operating multiple systems (e.g., CCTV, IDS, ACS, fire, HVAC, etc.). The process of training or re-training a single system is significantly easier and less costly than specialized training on each of the monitored systems. • By implementing an integrated approach, monitoring personnel can use a single workstation, versus the need for multiple computers and workstations for separate systems. This saves both the cost of the extra computers, GUIs, and peripheral devices, and the space required by equipment, which could be used to meet other operational needs.				
Power Resilience/Security	• Electronic security systems should be designed and installed with an appropriate level of power and backup. • Each individual panel or discrete device should be equipped with battery backup with a minimum 4 hours of storage capacity. Computers and other software services should be provided with an uninterrupted power supply in the event of main building power failure. All systems should be connected to either a secondary power feed/circuit (if available) or backup generator. Wiring to all devices should be in conduit and redundant wiring paths are preferred, if available. Security devices should be supervised and there should be an automatic notification on loss of a device. • All electrical panels should be locked and accessible only to authorized personnel. This is both a safety and security measure. • Data should be backed up based on the needs of the organization. The backup should include system set up, as well as the necessary amount of generated information (e.g., access events, video) required by the Owner or legislation. Backups should be regular and automated, not relying on an individual to remember to perform them. The security backup should be included as part of a regular information technology backup schedule.	• Although systems within the plant are limited (very little ACS, no IDS, underutilized CCTV/VMS), those that are in place include high quality platforms. Wiring to all devices is in conduit and end devices are supervised, as desired. Although control panels for security are located in locked rooms, they are not provided with tamper switches. • Electrical panels are not typically locked, although they are located in buildings that should be locked. This approach does not meet standard guidelines. • Power to the site is redundant. There are six generators available to address different areas of the plant. The generators are tested regularly.	• ID#71 - Panels are not locked. However, many are located in locked buildings. • ID#72 - Security devices are part of plant systems equipped with backup generator power. Uninterrupted power supply is available for all software related to security. • ID#73 - All wiring is in conduit. • ID#74 - There is no need for redundant wiring paths for the existing limited security installation. Redundant wiring should be considered as part of future security system installations. • ID#75 - Security devices are supervised. • ID#76 - Resilient power is provided via generators.	• **R27** - Ensure that all exterior panels include, at a minimum, a lock and chain or padlock.	• **R27** - High priority.
Water Quality Monitoring	• Water Quality Monitoring is driven by legislation and reporting requirements. It is incumbent on the operator to fully meet the requirements of their operating license.	• Regular and 24-hour sampling occurs at the RWQCP. Samples are collected from various locations across the plant and taken to the lab on site for processing. In addition, tegular readings are taken for turbidity and pH. The plant is fully meeting regulatory obligation relative to water quality monitoring.	• ID#64 – The plant fully meets the respective ANSI 57-10 Standard guideline.	• None.	• N/A.
SCADA Physical Security	• All SCADA equipment should be secured using physical and electronic measures. Panels/enclosures should be locked and equipped with tamper switches. Servers should be locked in a server room and monitored with ACS and CCTV.	• Enclosures on site are locked but do not have tamper switches. Most enclosures are located inside locked buildings. The server room is not a secure environment, relying solely on a keyed lock for protection.	• ID#77 - Enclosures are locked, and/or in locked rooms. • ID#78 - There are no tamper switches on SCADA enclosures. • ID#79 - All wiring is in conduit.	• **R28** - Add tamper switches to SCADA enclosures. This is also a recommendation addressed within the IDS section.	• **R28** - High priority.

5.7 Layer 5 - Operational Security

Layer 5 security includes the operational security efforts needed to best support the security profile generated through implementation of the first four layers. For example, the benefits of implementing a costly ACS or CCTV system cannot be fully realized without effective management of documented policies and procedures, such as system administration, training, auditing, monitoring, and change control documentation. There must also be an organizational approach associated with how visitors and contractors are managed/controlled, how keys are handled, and numerous other procedures that affect security at the site.

Operational security is frequently the most overlooked aspect of security planning within an organization. Very often, proper procedures and training are the most cost-effective security tool available to make a facility safe and secure. Implementing effective practices usually has very little capital cost and provides high returns.

Table 10 includes a detailed discussion of the Layer 5 security measures, including existing RWQCP conditions, a comparison to best practices, and recommendations to reduce risk. While operational security features are not included in the ANSI 57-10 Standard, the best practices within Table 10 are included for reference as the City enhances the security profile of the RWQCP.

Table 10 Layer 5 - Operational: Security Findings and Recommendations

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Security Policy	• The organization should have a documented security policy that is approved by executive management, readily available to all employees, and subject to periodic review and revision by executive management. Revisions to the document should be published, communicated, and distributed to all employees, accompanied by a revision checklist. The policy should provide authority to the appropriate personnel to develop, amend, review, and enforce security procedures in multiple domains. These domains are indicated below: – Corporate security policy is the high-level plan by which senior management expresses its commitment, delegates responsibility, establishes standards, and sanctions certain activities to protect the organization and its assets from harm. – The policy should demonstrate a commitment to future security within the organization by indicating the need to implement a long-term security master plan, with the goal of providing a safe and secure environment that protects both the people and assets of the organization.	• There is currently no existing security policy.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R29** - Develop and roll out Security Policy per Best Practices.	• **R29** - High priority. • Development of security policy and procedures can be accomplished quickly at reasonably low cost and will provide extensive benefits.
Security Procedures	• Security procedures describe the functionally relevant security activities to be undertaken by employees in their day-to-day work. They are instrumental in guiding employee behavior with respect to personal safety and security and in providing them with the information, tools, and support needed to act appropriately in the event of a threat. Some security procedures would have organization-wide application, while others would be site- or department- specific. All procedures that are in use should be available to all employees. Typically, this can be accomplished via an internal website. • The organization should have documented procedures governing the subjects outlined below. These procedures are detailed, step-by-step actions to achieve a certain task. They should explain clearly how policy guidelines will be implemented in the operating environment.	• There are minimal existing security procedures.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - Develop and roll out Security Procedures per Best Practices.	• **R30** - High priority. • Development of security policy and procedures can be accomplished quickly at reasonably low cost and will provide extensive benefits.
Background Checks	• Background checks should be performed on all employees, regular contractors, and vendors to reduce the risk of hiring or allowing access to a potentially dangerous persons. • Criminal record background checks should include a combination of local, state, national, and international checks, depending on the position and access of the applicant. In addition, persons in positions of trust should also have checks performed relative to credit, fraud, and education. It is not unusual for persons to misrepresent themselves when trying to obtain a new position. This is very often a difficult issue for Human Resources personnel. Despite best efforts, employers do not always know exactly who they are hiring. As employer liability continues to increase for incidents that occur within the workplace, information obtained on personnel is vital for both safety and security.	• Basic background checks are performed on new employees only.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.
Photo ID Badging	• Facility staff should be able to readily identify other staff, contractors, or visitors via photo ID badging. Employees and contractors issued badges should be subject to background checks and be required to sign an acknowledgement of the conditions of use to obtain the badge. Contractor badges should have an automatic expiration date. • Whenever a badge is provided to either an employee or a contractor, the receiver should be required to sign an acknowledgement of the conditions of use associated with the badge - including matters such as not loaning the badge, reporting it when lost or stolen, and using it only for authorized purposes.	• Badging is enforced to support the limited existing ACS. Photo ID badging for identification is not used.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices. • It is not uncommon for organizations of this size to not use photo IDs.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Contractor Controls	• Contractors should be issued badges with an automatic expiration date. They should be subject to background checks to receive their badges and be required to sign an acknowledgement of the conditions of use associated with the badge.	• Contractors are not issued badges with a defined expiration date.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.
Visitor Controls	• All visitors must be qualified before entering the site. All visitors must sign in and leave appropriate identification at the sign in. Visitors should not be allowed unescorted on the site.	• Visitors arrive at the main gate and must speak via intercom to either reception or the Control Room, who can provide entry. Visitors then are expected to sign in at the Reception area in the Admin/Lab Building. However, there is no real control over this procedure. Once allowed into the gate, the visitor could conceivably move about the site unencumbered. Visitors do not leave identification at sign in.	• **ID#14** - Visitors sign in.	• **R30** - Develop a written procedure regarding visitors and contractors, as part of the overall Security Procedures document. The procedure should include ensuring that visitor identification is checked.	• **R30** - See Security Procedures, above. • Refers to all policy/procedure development.
Key Control	• All keys and access cards that allow perimeter entry or access to restricted or critical areas should be controlled and stored in a secure manner. Keys should be issued only to those persons who can be entrusted with them and who have a legitimate and on-going need to access secure venues. Before an effective key control program can be established, every key to every lock used to protect a facility must be accounted for. Once an effective key control program has been instituted, positive control of all keys must be maintained. • Key issue records, key control cabinets, key inventory audits, and master key control are necessary ingredients in an effective key control program. Key and access card control can be maintained in several ways. The least efficient but most common method is the key log, typically a pen-and-paper exercise whereby all keys are centrally stored and signed out on an as-needed basis. The required personnel resources associated with this method generally make it the first gap in the security system. Specifically, it is too time consuming to expect key control to be maintained in this way. Instead, there are automated systems that can control access to keys and access cards and maintain tight control. • Similarly, issuing long-term use keys and access cards to new employees must be regulated and properly logged. As with ID badges, all recipients of keys and access cards must fully understand their appropriate use, that duplication is prohibited, and sign an acknowledgement of the terms and conditions associated with their use.	• The site currently has effective key control, based on an Assa-Abloy system with Grand Master hierarchy. Keys are signed out to individuals, with the approval of their manger, for the term of their employment. Spare keys and vehicle keys are kept in a lock box and tightly controlled by the key manager. A sign out is required to provide non-permanent keys to individuals. • The exception to the above statement is golf carts. They use a shared key and a golf cart was recently stolen and driven off the site. The golf cart keys were with the carts and unlocked.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R31** - Ensure all keys, including golf cart keys, are always secured.	• **R31** - High priority. • This is a low cost and very simple effort to implement.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Incident Reporting	• An organization should have a system available for proper and effective reporting and tracking of various types of incidents at the facility. • A proper incident reporting system that is easy to use and readily available should increase the likelihood of employees reporting matters that directly or indirectly affect the safety and security of the site. Incident reports allow the user to note trends in security matters on the site, and to possibly anticipate and thus prevent similar events.	• There is no formal automated incident reporting for security.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.
Change Control	• Change control procedures pertaining to the automated security systems should be developed and documented. • Change control is an integral part of any business process. Relative to security systems, any changes to cards, locks, cameras, or alarms should require managerial approval. There must also be an audit trail of these requests and approvals. Once the manager requests the change, the appropriate administrator should provide the required cards or changes. Change control should also include an audit process. • Changes to the physical system should be requested in writing and documented. This includes minor changes, such as changing the time that the intrusion system disarms. • When changes to the system are made, it is important to communicate them to the users.	• There is no existing formal change control at the site. This is primarily because the security systems are very limited. As they are further developed, a change control apparatus will be required.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.
Preventative Maintenance	• All electronic systems, including security systems, should have regularly scheduled preventative maintenance programs. The owner should require detailed reporting of the program. • A security system is composed of electronic and mechanical parts, each with a mean time to repair that must be observed. Failure of any one system component can compromise the entire system and the security of everyone and everything that it protects. An electronic security system that is not maintained on a regular basis will soon fall into disrepair and will not provide the functionality it is designed for, ultimately costing the organization significant capital outlay. • Maintenance should be performed on a scheduled basis. Performing maintenance twice per year is typically sufficient to maintain the types of systems being recommended for this facility. The maintenance would include matters such as cleaning and adjusting cameras, testing preset locations on PTZ cameras, and fine-tuning and recalibrating fence alarms. A full preventative maintenance package should be detailed in the final specifications for the system. The system integrator should be capable of providing this twice-yearly program. However, site personnel could be trained to provide the required maintenance as well. The critical issue is to ensure that, no matter who is responsible, maintenance is performed on a schedule and maintenance records are kept on file.	• Currently, existing security devices are not part of a preventative maintenance program. Repairs/programming adjustments are made on an as needed basis. For the limited systems currently in place, this approach is sufficient. As more complex systems are introduced, there will be a need for a more defined preventative maintenance program.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.
Security Awareness Training	• Regular training sessions should be delivered in various formats to ensure that the staff are aware of their security responsibilities and are equipped with the proper information to meet these responsibilities. • An important component of any successful security plan is ensuring those involved in the plan understand that security is everyone's responsibility. A security practitioner can design the perfect system at the perfect price, but if the users see these measures as an inconvenience rather than a benefit, they can and will compromise the system. Therefore, training and awareness are vital components of the security profile of a facility.	• There is no security awareness training on a regular or organized basis, which has resulted in issues such as tailgating at the main gate (i.e., when a legitimate vehicle entry is made, but the driver does not wait for the gate to close behind them to prevent unauthorized vehicles from following).	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.

Security Category	Best Practice	Existing Condition	ANSI 57-10 Security Measure Reference	Recommendation	Priority
Performance Measurement	• All elements of the security program should be audited regularly against a baseline performance. This applies to physical, electronic, and operational/procedural security.	• There is no performance measurement system in place. As security at the site is further developed, such an system will be required.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.
Lock Up	• Building perimeter doors should be locked at the end of the business day. If possible, doors should be capable of auto-locking via the ACS. The roving patrol guard should always rattle-check doors. Individual office doors should be the responsibility of the user.	• Employees are expected to lock doors and they are generally checked at night (although there is no formal process). During the day, numerous doors are left open for convenience. Addition of an ACS would reduce this vulnerability.	• There is no ANSI 57-10 reference for this operational security element. Alternatively, this evaluation reviewed adherence to Best Practices.	• **R30** - See Security Procedures.	• **R30** - See Security Procedures, above.

Section 6

RECOMMENDATIONS AND NEXT STEPS

The recommendations provided in Section 5 for each layer of security have been organized into a total of seven security projects based on the scope and priority of each recommendation. Project implementation can be completed in phases over several years to improve the security profile at the RWQCP to meet ANSI 57-10 guidelines and best practice recommendations. Table 11 summarizes the recommendations included within each of the proposed security projects. The "R" number in the left hand column refers to the recommendation presented in the tables in Section 5.

Table 11 Security Assessment Recommendations

No.	Recommendation	Detail Reference	Priority
Interim Security Improvements – Mobile CCTV			
R7	Employ ECAMSECURE mobile units to meet immediate security needs. Refer to Section 5.6 and Appendix C for more details on implementation. Project 2, below, supersedes this interim solution when complete.	Table 6 - Intrusion Detection	High
Project 1 - Plant Fencing and CPTED Improvements			
R1	Improve fencing in northeast.	Table 6 - Perimeter Fencing	Medium
R2	Provide concrete barrier under fencing in several areas.	Table 6 - Perimeter Fencing	High
R3	Add fencing/gate near septic drop area.	Table 6 - Gates	High
R4	Clear vegetation along perimeter fence.	Table 6 - CPTED	Medium
R5	Clear (exterior) materials along perimeter fence.	Table 6 - CPTED	Medium
R9	Clear vegetation.	Table 7 - CPTED	Medium
Project 2 - CCTV Perimeter Protection			
R7	Add perimeter protection using CCTV (thermal and visible).	Table 6 - Intrusion Detection	High
R8	Provide alarm assessment capability on perimeter.	Table 6 - Alarm Assessment	High
R20	Add system-wide monitoring capability via exception-based monitoring.	Table 9 - System Monitoring	High
R24	Develop and implement comprehensive CCTV platform to address surveillance, alarming, alarm assessment, and investigative capabilities site wide.	Table 9 - CCTV and VMS Platform	High
Project 3 - Internal Surveillance/IDS with Video			
R12	Add CCTV intrusion detection for Layer 2.	Table 7 - Intrusion Detection	High

No.	Recommendation	Detail Reference	Priority
R13	Provide alarm assessment capability for Layer 2.	Table 7 - Alarm Assessment	High
Project 4 - Access Control and Intrusion Detection			
R15	Add internal glassbreaks on windows.	Table 8 - Windows/Openings	Medium
R17	Add ACS within the Admin Building to separate the common area from the interior.	Table 8 - Separation	Medium
R18	Add ACS to Server Room and Control Room.	Table 8 - Separation	High
R19	Add IDS to building perimeter points.	Table 8 - Intrusion Detection	Medium
R22	Provide platform to expand ACS to encompass all critical buildings and structures.	Table 9 - ACS Platform	High
R25	Develop and implement comprehensive IDS program for all layers. Utilize CCTV where appropriate to limit duplication of cost and effort.	Table 9 - Intrusion Alarming Platform	High
R26	Ensure integration of all security systems as they are built out.	Table 9 - System Integration	Medium
Project 5 - Security Policy and Procedures			
R21	Develop alarm response protocols.	Table 9 - Alarm Response	High
R29	Develop and deliver Security Policy.	Table 10 - Security Policy	High
R30	Develop and deliver Security Procedures documentation for all aspects noted in Table 12.	Table 10 - Multiple	High
R31	Ensure golf cart keys are properly secured.	Table 10 - Key Control	High
Project 6 - Miscellaneous Physical Security Upgrades			
R6	Discuss adding signs to address potential liability concerns.	Table 6 - Signs	Low
R10	Replace building signs.	Table 7 - CPTED	Low
R11	Add bollards at key electrical equipment (external).	Table 7 - Equipment	Low
R14	Provide security hinges for all doors.	Table 8 - Doors/Locks/Hinges	Low
R16	Repair access ladders.	Table 8 - Windows/Openings	Medium
R27	Lock all exterior panels with chain and/or padlock.	Table 9 - Power Resilience/Security	High
Project 7 - Miscellaneous Electrical Security Upgrades			
R23	Activate and use gate exit readers.	Table 9 - ACS Platform	High
R28	Add tamper switches to all SCADA enclosures.	Table 9 - SCADA Physical Security	High

Table 12 includes a planning level cost overview and recommended implementation schedule for each security project. In general, projects recommended for short-term implementation include high priority or low cost work items that can significantly improve the RWQCP security profile. Note that the suggested implementation schedule begins with Project 7 identified in Table 11. An itemized breakdown of the costs included for each recommendation and project is included in Appendix D.

Note too that these planning level costs represent a high-level budgetary estimate based on Carollo's understanding of the design effort and implementation costs required at the project location. Costs will need to be refined during the design phase of each project based on the ultimate design/installation and market conditions at the time of the project.

Carollo has no control over variances in the cost of labor, materials, equipment; nor services provided by others, contractor's means and methods of executing the work or of determining prices, competitive bidding or market conditions, practices or bidding strategies. Carollo cannot and does not warrant or guarantee that proposals, bids or actual construction costs will not vary from the costs presented as shown.

The cost estimates represent a Class 5 budgetary estimate as defined by the AACE International. Typical accuracy for Class 5 Estimates is expected to be in the range of -30 to +50 percent. It should be noted that pricing accuracy is time sensitive and, based on current market conditions, may degrade over relatively brief periods of time. Pricing updates should be made regularly to increase the overall reliability of the cost estimates.

Table 12 Security Project Implementation Summary

Implementation Schedule	Project	Project Cost[1][2]
Present	Interim Security Improvements – Mobile CCTV	$254,500[3]
2023	Project 7 - Miscellaneous Electrical Security Upgrades	$20,000
2023	Project 5 - Security Policy and Procedures	$50,000
2023-2024	Project 2 - CCTV Perimeter Protection	$2,340,000
2024-2025	Project 4 - Access Control and Intrusion Detection	$790,000
2025	Project 1 - Plant Fencing and CPTED Improvements	$220,000
2025	Project 3 - Internal Surveillance/IDS with Video	$200,000
2025	Project 6 - Miscellaneous Physical Security Upgrades	$120,000
	TOTAL	**$3,994,500[4]**

Notes:
(1) Costs are based on October 2022 market conditions and include the following: 30 percent contingency, 9.5 percent taxes, 30 percent Engineering/Admin Fees, 18 percent Contractor's Overhead and Profit. Escalation to mid-point of construction has not been included.
(2) The project costs were rounded up to the nearest $10,000.
(3) Approximate cost for interim CCTV solution is for one year of mobile CCTV units, based on a monthly operating cost of $21,210 as provided by ECAMSECURE. Actual cost could be less or more depending on completion of Project 2, which will supersede the interim mobile CCTV solution. Refer to Appendix C for more details.
(4) As noted above, total implementation costs include 1 year of interim mobile CCTV units. This number will change based on actual mobile CCTV timeframe (pending implementation of Project 2).

Appendix A

EXTERIOR LIGHTING STUDY

Appendix A
EXTERIOR LIGHTING STUDY

Lighting is an important component of a facility's security profile. Lighting in Layer 1 (perimeter) and Layer 2 (clear zone) can increase the chances of a criminal being caught and improve general staff safety or operations. Members of the assessment team visited the Regional Water Quality Control Plant (RWQCP) site on August 17, 2022, to collect light intensity data and identify supplementary lighting required to support plant operations and staff safety.

Lighting was evaluated from multiple perspectives:

- Security (deterrent, detection of intruders, adequate lighting to support closed-circuit television [CCTV]).
- Staff safety (ability to identify and address hazards).
- Operations (visibility during evening operations).

The results and recommendations from the assessment are provided in this appendix.

Methodology

The exterior lighting study was conducted in the evening when there was no sunlight available. The intent of the study was to measure the amount of lighting provided by the existing RWQCP site lights. Lighting measurements were collected along the plant perimeter and at critical operation areas within the plant using a handheld Extech LT300 light meter. The Extech LT300 light meter utilizes a remote light sensor connected with a 12-inch coiled cable to measure light, with a range up to 40,000 footcandles (fc) (or 400,000 Lux). Readings for this project were taken in fc.

Generally, the lower the light reading, the less adequate light is available. Readings of .01 to .03 are virtual darkness to the naked eye. Readings up to about 1.0 are providing more and more visibility for safety purposes. Beyond 1.0 there is little difficulty in presenting the human eye with ample information. However, this representation must consider the use of the visible light. If visible light is in place primarily as a safety or operational measure, the requirements are different than lighting for security or CCTV purposes. The quality of CCTV presently is such that there are no areas of the plant that could not receive adequate CCTV performance, even if that means the use of thermal imaging to reach this standard. See the CCTV memo for further detail on this subject.

Where the intent of the light is solely to assist in safety or operational assistance, a minimum of .05 fc should be considered. It is also important to note that lighting can be a useful crime deterrent. Levels above 1.0 fc can generally be expected to act as something of a deterrent.

Results

The lighting measurements collected as part of the study are provided on Figure A.1. The Figure utilizes a base map generated by MWH as part of a lighting study completed for the RWQCP in 2014. All lighting measurements are presented in fc.

Color Legend:

- Existing Site/Area Lighting (at the time of the MWH Study)
- Project T-46 Site/Area Lighting
- Project T-46 Process (Switched) Lighting
- Proposed Perimeter Security Lighting (from MWH Study)
- Proposed High Mast (HM) Area Lighting (from MWH Study)
- Light Measurements Collected August 17th, 2022

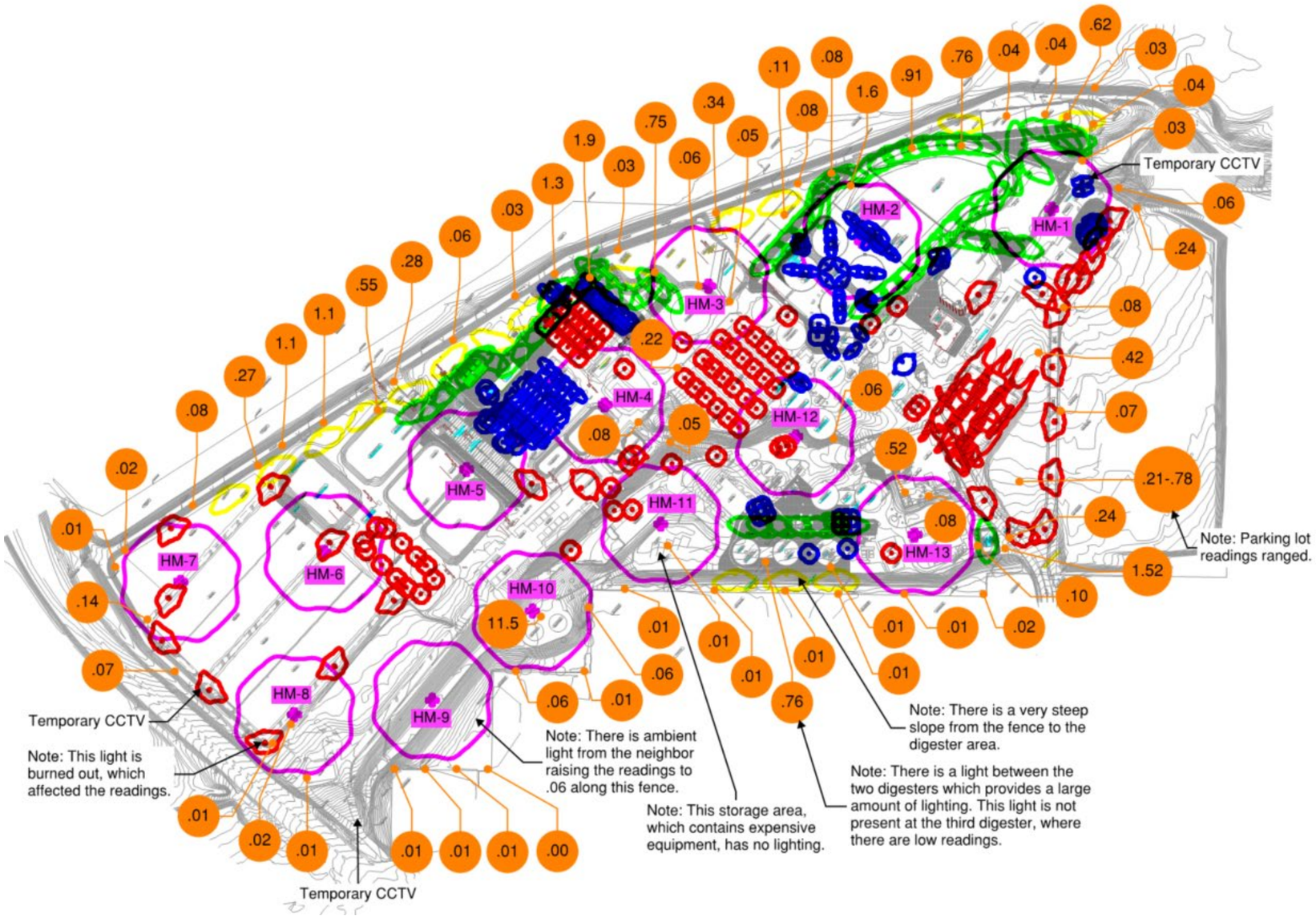

Figure A.1 RWQCP Site Lighting Measurements Collected 8/27/22

Other observations from the exterior lighting study include:

- The **existing area lighting** provides ample illumination in the areas where it exists.
- The **perimeter lights** on the northern boundary are effective. The darkest areas, with readings of 0.03, were midway between light posts. However, lighting in these areas was still adequate to support CCTV and other surveillance. There is no lighting installed on the south perimeter.
- **High mast lighting** was proposed in the MWH study to overcome challenges associated with steep slopes in areas of the site. The west side of the plant is not well lit. However, staff do not frequent those areas because there are no treatment processes in this area. If the effective security measures detailed in the Security Assessment Study (including thermal and pan-tilt-zoom cameras) are installed, several of the proposed high mast lights may not be necessary. The high mast lighting areas are summarized below:
  - HM-1 & HM-2: There is significant existing light in these areas. The addition of new lights in these locations is not critical.
  - HM-3: This area is not well lit and does include several structures. The addition of a new high mast light in this location may be beneficial, but is not necessary if effective perimeter security, as described in the Security Assessment Study, is implemented.
  - HM-4: This area is well lit and includes several structures. The addition of new lights in this location is not critical.
  - HM-5 & HM-6: These areas include the drying beds, which are not frequented by staff, especially during the evening hours. The addition of new lights in these locations is not critical.
  - HM-7 & HM-8: These areas are very dark and include significant debris that can be dangerous to staff. The addition of new lighting in these areas is recommended to support staff safety and operations.
  - HM-9: This is a notable area of concern, having been the entry point for several site break-ins in the past. The addition of new lighting in this area is recommended to support staff safety and operations.
  - HM-10: Lights have been added to this area, which provide excellent lighting north of the tanks. The addition of lighting to cover the slope south of the tanks would also be beneficial.
  - HM-11: This area, where expensive equipment is stored, is poorly lit. The addition of new lighting in this area is recommended to protect plant assets. Providing lighting in locations HM-10, 11, and 13 may limit the need for thermal CCTV, leading to possible cost savings.
  - HM-12: There is adequate existing lighting in this area to support operations. The addition of new lights in this location is not required/recommended.
  - HM-13: Ample lighting is available from the nearby entrance in this location. The addition of new lights in this area is not critical, although it may be beneficial to provide more lighting in the southeast corner, near the gate, if this area is of concern to staff.

Recommendations

Based on the results of the exterior lighting study, Carollo recommends the following improvements at the RWQCP to support security, staff safety, and operations. Note that several of the lighting recommendations should be evaluated in conjunction with the recommendations outlined in the Security Assessment Study.

- The existing lighting in most areas of the RWQCP is adequate to support operations and staff safety. Ample lighting is available at the site entrance and at critical processes, such as the digesters and clarifiers. There are several areas within the plant, particularly along the south perimeter, that are not well lit. However, not all of these locations require the installation of new lights, since these areas either include processes that do not require evening operations (e.g., drying beds) or can be effectively addressed through thermal or infrared cameras.
- To support plant operations and staff safety, new lighting should be installed at the following location within the RWQCP site:
  - The west perimeter (HM-7, HM-8, and HM-9) – this area contains significant debris that can be dangerous to staff. In addition, the perimeter is a notable area of concern, having been the entry point for several previous site break-ins. Improved lighting here would assist as a deterrent, although it is not required to assist the detection function. The recommendation for thermal imaging will address the detection and assessment components. If ample visible light is added here, the recommendation for the use of thermal can be altered to low light CCTV in place of thermal.
- To support facility security, new lighting should be installed at the following location within the RWQCP site:
  - Storage Area (HM-11) – this area contains expensive equipment that should be better protected. Visible light here would be a strong deterrent, especially as the area is relatively close to manned locations (as opposed to the dark areas on the west perimeter).
- As noted previously, site lighting should be closely coordinated with the Security Assessment Study, which recommends installation of CCTV throughout the plant site. In areas where lighting is needed to support staff safety or operations, the proposed lighting may be adequate to support CCTV and eliminate the need for more expensive, thermal CCTV. In other areas, staff may choose to install visible lighting.

Appendix B

PHOTO LIBRARY

Appendix B

PHOTO LIBRARY

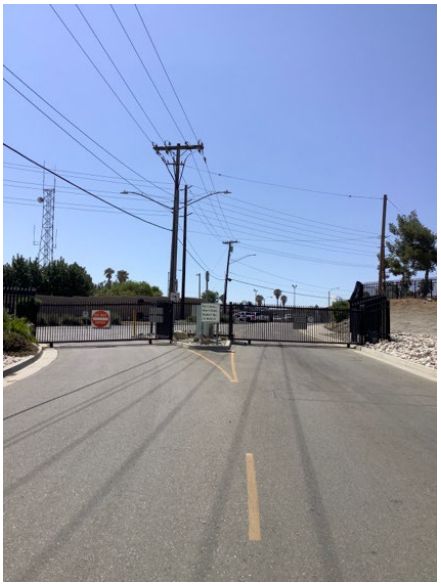

Photo 1: Layer 1 - Main gate is well lit. There have been concerns with tailgating as the exit gate does not use the available card readers. There is no sally port, however such a device is unnecessary here.

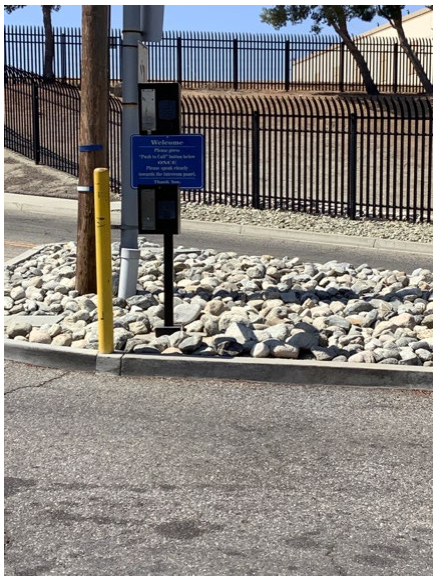

Photo 2: Layer 1 - Good use of bollard to protect the entry and intercom.

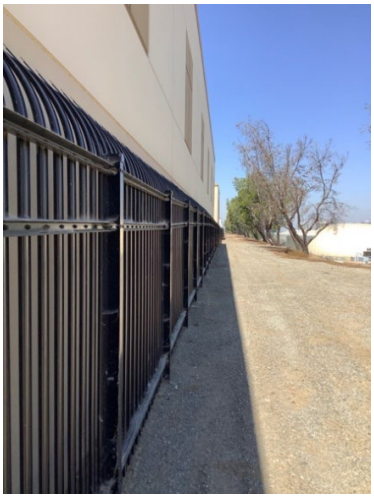

Photo 3: Layer 1 - The fencing on the south side shown here is easily defeated by entering via the nearby buildings, which are not owned or controlled by RWQCP.

Photo 4: Layer 1 - Fence is defeated by equipment piled outside it.

Photo 5: Layer 1 - CPTED concerns with vegetation on perimeter. Allows entry, hiding spots, and inhibits surveillance.

Photo 6: Layer 1 - CPTED concerns with vegetation on perimeter. Allows entry, hiding spots, and inhibits surveillance.

Photo 7: Layer 1 - CPTED and other concerns. There is a person living in an uncontrolled area of brush just outside the fence line in the southwest. There is no surveillance or alarming available.

Photo 8: Layer 1 - The main fence is effective and meets best practices. The secondary fence shown here is unnecessary.

Photo 9: Layer 1 - Padlocks on man gates are not very strong and can be cut.

Photo 10: Layer 1 - Example of effective fence, lighting, and signs on the north perimeter.

Photo 11: Layer 1 - Fencing around the east perimeter does not match the very strong fencing elsewhere. The razor wire helps, however the fence itself is low (6-ft) and can be cut. There is no effective alarming in the area.

Photo 12: Layer 2 - Generators near the main gate are properly enclosed.

Photo 13: Layer 2 - Tank ladder is insecure.

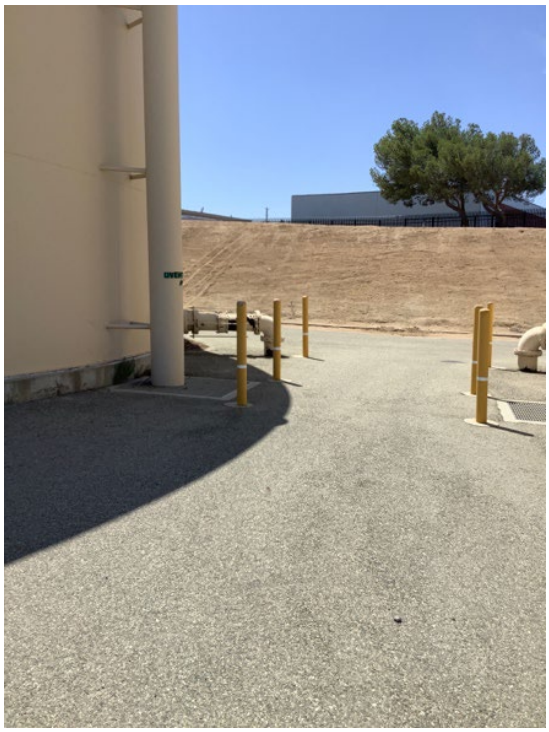

Photo 14: Layer 2 - Bollards protecting outdoor critical equipment.

Photo 15: Layer 2 - Effective lighting at the north generators.

Photo 16: Layer 2 - These transformers are padlocked, although not caged. This is effective.

Photo 17: Layer 3 - Typical process area door. Metal in metal frame, however this door has no astragal.

Photo 18: Layer 3 - Propped doors create risk.

Photo 19: Layer 3 - Doors to some critical areas are left open to provide ventilation. This is a vulnerability, and there is a reliance on human interaction to ensure they are locked after hours.

Photo 20: Layer 3 and Layer 5 - There are numerous cameras on site that could be effectively tasked to security purposes.

Photo 21: Layer 3 - These doors are an example of strong physical security for entry points. They are metal, in metal frames, and have a full astragal.

Photo 22: Layer 3 - Windows and doors with windows are too easily circumvented.

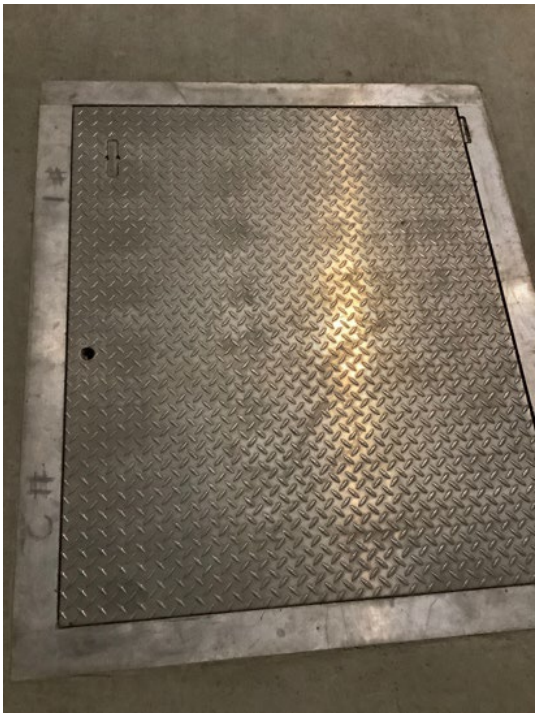

Photo 23: Layer 4 - Hatches were found to be locked.

Photo 24: Layer 4 - There is surveillance capability, but it is not being optimally employed.

Photo 25: Layer 5 - Exterior accessible panels should be locked.

Appendix C

CCTV UNIT EVALUATION

City of Riverside
Regional Water Quality Control Plant
Security Assessment Study

Technical Memorandum
CCTV UNIT EVALUATION

FINAL | January 2023

carollo

City of Riverside
Regional Water Quality Control Plant
Security Assessment Study

Technical Memorandum
CCTV UNIT EVALUATION

FINAL | January 2023

Contents

Tables

Figures

Section 1

PURPOSE

The City of Riverside's (City) Regional Water Quality Control Plant (RWQCP) is equipped with a variety of fixed and pan-tilt-zoom closed-circuit television (CCTV) units that support process and other building access security functions. However, the existing units do not provide perimeter security for the facility.

The City is currently testing three CCTV rental units to supplement perimeter security and address security problems along sections of the plant perimeter. These units are on a 30-day trial rental program from ECAMSECURE and are intended to provide a temporary solution for perimeter security. The purpose of this technical memorandum (TM) is to help the City determine the value of extending the rental period, pending a permanent CCTV/perimeter security solution at the RWQCP.

Section 2

CURRENT TEMPORARY CCTV INSTALLATION

Each of the three ECAMSECURE rental units deployed on site consists of a camera, battery power, lighting, and a cellular card for transmitting signal. The units are mobile (mounted on a trailer) and can be easily moved to any area of the RWQCP. The units can view an area up to 150 feet away, with a 90-degree field of view. The current locations of the three mobile units are shown on Figure 1.

Figure 1 Locations of the Temporary CCTV Units

The units are equipped with Axis model cameras. These systems are not intended for low-light environments and require the presence of visible light to support proper functionality. The cameras include intelligent video that triggers an alarm to a third-party monitor, when an event (usually defined as motion) occurs within a certain period. This third-party then notifies RWQCP personnel through a call-out list.

The existing approach is appropriate for its limited scope. The Axis cameras are excellent quality, and field testing demonstrated that the alarming and monitoring functions are being handled properly. The primary concern associated with the installation is that the current configuration controls very little of the perimeter. The site perimeter is well over 8,000 feet. The three rental units cover only 5 percent of the perimeter. Using these same units/approach to cover the entire perimeter would require over 50 installations. This is not a viable solution from a cost or operational perspective.

In addition, the installations are easily identified by an outsider, as they use bright lighting to assist the visible light cameras in identifying events. This issue is discussed in additional detail in Section 3.

Section 3

THERMAL IMAGING

Until a permanent CCTV protection system is implemented, the City is seeking a temporary solution to address their plant perimeter concerns.

One potential solution to the cost challenges associated with implementing the current ECAMSECURE rental units on a larger scale is to provide greater ranges for the CCTV units. Using thermal imaging units, rather than standard visible light or infrared (IR) cameras, adds significant range to the alarmed field of view. There are thermal imagers that can "see" up to several kilometers in open space.

The primary advantage of cameras that create images using visible light, such as conventional surveillance or IR-illuminated cameras, is that the images they create are recognizable and easy to interpret. This familiarity makes them a more comfortable choice for end users. However, these cameras have inherent challenges when it comes to detection - primarily that visible light cameras are reliant on the amount of available light. In sunshine or a brightly lit areas, visible light cameras perform very well. In situations where lighting is less than ideal, objects can appear faint or not appear at all. Visible light cameras are also limited by visual contrast. Because they capture only visible light, the cameras can be deceived by visual camouflage or other factors, such as trees and shadows.

Typically, a thermal imager is more reliable than a visible light or IR camera. The thermal unit is less hindered by rain, snow, fog, or other inclement weather. These conditions can limit the range of a thermal unit, but are unlikely to block the transmission of light entirely. Thermal imaging cameras equipped with onboard video analytics are capable of classifying human or vehicular perimeter intrusions, resulting in fewer false alarms.

The primary drawback of thermal imaging is that the unit is designed to identify differences in temperature, which show up in the image as shades of black and white. Under ideal conditions, a visible light camera can identify not only an event, but can provide valuable information such as the color of clothes being worn or the identity of an intruder. This level of detail is not available with thermal imaging units.

Figure 2 includes an example of an image provided by a thermal unit. It is difficult to determine the make and model of the car, the license plate, the color of jacket, or facial features of the person in the image. However, in many cases, this level of detail is not critical. The ultimate goal of perimeter detection is to identify an intrusion - not necessarily to identify the intruder. The capability to accomplish this at long range enhances the perimeter security of the RWQCP and reduces the capital and operational costs.

Figure 2 Example Thermal Unit Image

Figure 3 and Figure 4 further demonstrate the benefits of using thermal imagery. On Figure 3, the image on the left was taken with an IR camera, while the image on the right was taken with a thermal imager. On Figure 4 the image on the left was taken with a visible light camera, and the image on the right was taken with a thermal imager. The advantages of thermal in these applications is clear - alarms would be created when the intruders are detected, and RWQCP personnel would be contacted by the third-party.

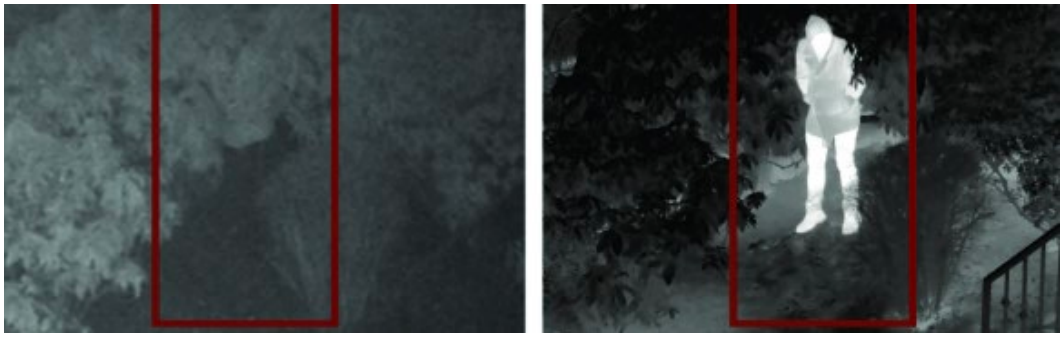

Figure 3 Infrared Versus Thermal Imager

Figure 4 Visible Light Camera Versus Thermal Imager

ECAMSECURE indicated that they are prepared to install Axis thermal imaging on the mobile CCTV units, rather than the currently installed short-range visible-light cameras. While there are several companies who provide thermal cameras, not all are of the same quality. Our team has had positive experience with the Axis units and believes this is an appropriate product for the application.

The proposed units would include two thermal cameras, local power, a visible light camera, and a network card. No lighting would be required. The thermal units would be placed back-to-back, each with a range of 600 feet. The visible light camera would be deployed to cover the dead area created by the back-to-back thermal configuration. Consideration was given to using single camera units in an overlapping line. This would eliminate dead spots, but would require more mobile trailers, power, and transmission.

Section 4

INTERIM TERM SOLUTION

It will likely take a year or more before a permanent perimeter camera system can be installed. In an effort to provide an interim perimeter security solution, we recommend employing thermal imaging units through the ECAMSECURE model. Figure 5 provides a plant layout and potential locations for the units as part of this temporary solution.

Approximate distances are provided on Figure 5 in yellow at various points around the perimeter. The blue circles indicate the seven proposed thermal unit locations, each of which would include two thermal sensors, two fixed HiRes Axis cameras, alert strobe lights, complete solar power, one warning speaker, one mounting trailer, remote live access, and up to ten days of local storage for 24 hours per day, 7 days per week continuous recordings. The blue line emanating from each of the circles represents the estimated detection range of the Axis thermal imagers - approximately 600 feet in each direction.

This design concept provides CCTV coverage for essentially the entire perimeter. The only location that is not well covered in this design concept is the front gate area, which is presently well lit and has ample local CCTV coverage. A budgetary cost provided by ECAMSECURE for this proposed design concept is provided in Table 1.

Table 1 Budgetary Estimate for the Recommended Interim Perimeter Security Solution

Item	Unit Cost	Cost ($/month)	Cost ($/year)
CCTV Unit(4)	$2,920/unit/month	20,440(1)	245,280(1)
Monitoring Services	$770/month	770	9,240
One-Time Setup Cost	$800	N/A	N/A
Total(2)		$21,210	$254,520(3)

Notes:
(1) Cost assumes installation of the seven units proposed.
(2) The total cost per month and total cost per year do not include the one-time setup cost of $800.
(3) Leasing for a year can produce a discount of 10-11 percent.
(4) There is a lease to purchase option available for the CCTV units. It is recommended that these units be used as a temporary measure only, unit a permanent CCTV/perimeter security solution is installed at the RWQCP. However, if the City should wish to lease to purchase, the CCTV units could be re-tasked for the permanent installation.

While this approach is far more cost-effective than the current visible light solution, it is still likely a relatively costly endeavor. However, there are several ways to reduce the potential costs.

- The recent installation of lighting along the north perimeter would support the use of non-thermal cameras in that area. Bosch, Samsung, Axis, Avigilon, and other manufacturers provide excellent quality perimeter cameras that can operate effectively in low light. Using these cameras, in lieu of more costly thermal units for well-lit areas, would reduce capital costs, without impacting the long-term solution.
- The thermal units could be installed incrementally, depending on local circumstances and concerns. For example, the City could prioritize installing the camera unit shown at Location 3 to replace two of the existing mobile units. This approach would provide perimeter coverage for the western perimeter, where lighting is the poorest.

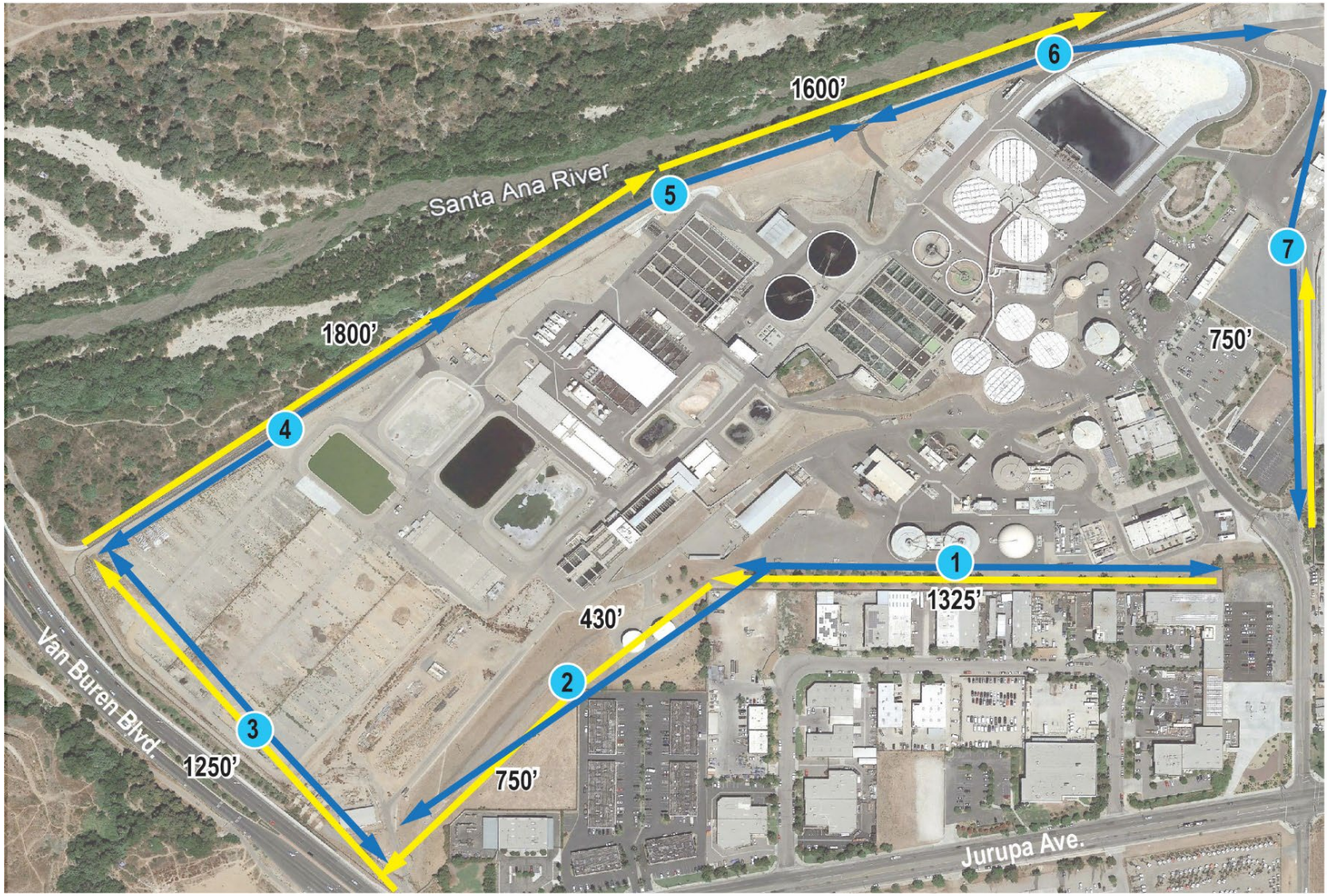

Figure 5 Proposed Locations for Thermal Imaging CCTV Units

Section 5

SUMMARY

The optimum long-term solution to provide appropriate perimeter security at the RWQCP will include installation of permanent technology to guard the fence line. This will be a recommendation in the forthcoming security assessment study. In the interim, employing the ECAMSECURE mobile units will meet the immediate security needs and concerns of the City. The units should be equipped with thermal devices, which will provide a more efficient and cost-effective way to combat intrusions along the perimeter (versus visible light cameras). Depending on available budget, the installation can be phased to address the most problematic areas of the perimeter first.

Appendix D

SECURITY PROJECTS BUDGETARY ESTIMATE

Riverside RWQCP
Security Recommendation Implementation
Conceptual Project Cost Breakdown Table

Asset /Project	Applicable Recommendations	Security Costs						Project Cost by Asset		
		Type	Units	Qty	Install Factor	Cost/Unit	Subtotals	Fee type	Percentage	Cost
Project 1 - Plant Fencing and CPTED Improvements	R1	Add wrought iron fencing in designated area Plant perimeter NE.	lf	750	1.2	$ 100	$ 90,000	Combined Subtotal		$102,400
	R2	Add concrete barrier under fence in designated areas Plant perimeter	each	2	1.2	$ 1,000	$ 2,400	Contingency	30%	$30,720.0
	R3	Add gate and fence separation from Septic drop off area	lump sum	1	1.0	$ 5,000	$ 5,000	Tax	9.5%	$12,646.40
	R4, R5, R9	Vegetation clearance	lump sum	1	1.0	$ 5,000	$ 5,000	Engineering/Admin	30%	$43,729.9
								Contractor Overhead/Profit/Fees	18%	$26,237.95
		Subtotal					**$ 102,400**	**TOTAL**		**$220,000**
Project 2 - CCTV Perimeter Protection	R7	Thermal Cameras	each	14	1.2	$ 8,500	$ 142,800	Combined Subtotal		$1,110,460
	R8	PTZ Cameras	each	8	1.2	$ 5,500	$ 52,800	Contingency	30%	$333,138.0
	R20	Video Servers, Licenses, & Storage	lump sum	1	1.0	$ 15,000	$ 15,000	Tax	9.5%	$137,141.81
	R24	Poles	each	9	1.2	$ 4,000	$ 43,200	Engineering/Admin	30%	$474,221.9
		Ductbank	lf	9000	1.3	$ 50	$ 585,000	Contractor Overhead/Profit/Fees	18%	$284,533.17
		Programming R24	lump sum	1	1.0	$ 5,000	$ 5,000			
		Security Network Switches	each	4	1.3	$ 2,000	$ 10,400			
		Misc. Electrical, Instruemntation, and Controls	%	0.3	1.0	$ 854,200	$ 256,260			
		Subtotal					**$ 1,110,460**	**TOTAL**		**$2,340,000**
Project 3 - Internal Surveillance / IDS With Video	R12, R13	Add internal PTZ integrated to ACS / IDS	each	10	1.3	$ 5,500	$ 71,500	Combined Subtotal		$92,950
		- building mounted						Contingency	30%	$27,885.0
		- servers / storage as part of Project 2						Tax	9.5%	$11,479.33
		- Integration						Engineering/Admin	30%	$39,694.3
		Misc. Electrical, Instruemntation, and Controls	%	0.3	1.0	$ 71,500	$ 21,450	Contractor Overhead/Profit/Fees	18%	$23,816.58
		Subtotal					**$ 92,950**	**TOTAL**		**$200,000**
Project 4 - Access Control & Intrusion Detection	R17	Control Panels	each	6	1.3	$ 2,800	$ 21,840	Combined Subtotal		$371,852
	R18	Servers, Software, Licenses	lump sum	1	1.0	$ 15,000	$ 15,000	Contingency	30%	$111,555.6
	R22	Card Reader Doors	each	30	1.3	$ 4,500	$ 175,500	Tax	9.5%	$45,923.72
	R26	I/O Boards	each	6	1.3	$ 2,000	$ 15,600	Engineering/Admin	30%	$158,799.4
	R15, R19	IDS component - devices	each	50	1.3	$ 500	$ 32,500	Contractor Overhead/Profit/Fees	18%	$95,279.64
	R25	Security Network Switches	each	6	1.3	$ 2,000	$ 15,600			
		Programming Integration	lump sum	1	1.0	$ 10,000	$ 10,000			
		Misc. Electrical, Instruemntation, and Controls	%	0.3	1.0	$ 286,040	$ 85,812			
		Subtotal					**$ 371,852**	**TOTAL**		**$790,000**
Project 5 - Security Policy and Procedures	R21, R29, R30	Develop and Deliver policy / procedure documents.	lump sum	1	1.0	$ 20,000	$ 20,000	Combined Subtotal		$20,000
	R31	Ensure golf cart keys are properly secured (no additional cost)	-	-	-	-	-	Contingency	30%	$6,000.0
								Tax	9.5%	$2,470.00
								Engineering/Admin	30%	$8,541.0
								Contractor Overhead/Profit/Fees	18%	$5,124.60
		Subtotal					**$ 20,000**	**TOTAL**		**$50,000**
Project 6 - Miscellaneous Physical Security Upgrades	R11	Bollards	each	20	1.2	$ 1,500	$ 36,000	Combined Subtotal		$53,500
	R14	Replace Hinges	each	100	1.2	$ 100	$ 12,000	Contingency	30%	$16,050.0
	R16	Repair Access Ladders	lump sum	1	1.0	$ 2,500	$ 2,500	Tax	9.5%	$6,607.25
	R27	Lock External Panels	lump sum	1	1.0	$ 500	$ 500	Engineering/Admin	30%	$22,847.2
	R6, R10	Site Signage	lump sum	1	1.0	$ 2,500	$ 2,500	Contractor Overhead/Profit/Fees	18%	$13,708.31
		Subtotal					**$ 53,500**	**TOTAL**		**$120,000**
Project 7 - Miscellaneous Electrical Security Upgrades	R23	Activate Reader Out for Gates (Ianor)	lump sum	1	1.0	$ 500	$ 500	Combined Subtotal		$5,720
	R28	Tamper Switches	each	15	1.3	$ 200	$ 3,900	Contingency	30%	$1,716.0
		Misc. Electrical, Instruemntation, and Controls	%	0.3	1.0	$ 4,400	$ 1,320	Tax	9.5%	$706.42
								Engineering/Admin	30%	$2,442.7
								Contractor Overhead/Profit/Fees	18%	$1,465.64
		Subtotal					**$ 5,720**	**TOTAL**		**$20,000**
TOTALS		**SECURITY IMPROVEMENTS SUBTOTAL**					**$1,756,882**	**OVERALL TOTAL**		**$3,740,000**

The cost estimate herein is based on our perception of current conditions at the project location. This estimate reflects our professional opinion of accurate costs at this time and is subject to change as the project design matures. Carollo Engineers have no control over variances in the cost of labor, materials, equipment; nor services provided by others, contractor's means and methods of executing the work or of determining prices, competitive bidding or market conditions, practices or bidding strategies. Carollo Engineers cannot and does not warrant or guarantee that proposals, bids or actual construction costs will not vary from the costs presented as shown.

This estimate represents a Class 5 budgetary estimate as defined by the Association for the Advancement of Cost Engineering (AACE) International. Typical accuracy for Class 5 Estimates is expected to be in the range of -30 to +50 percent. Consumers of construction cost estimate data should be advised that pricing accuracy is time sensitive and will degrade over relatively brief periods of time. Pricing updates should be made regularly to increase overall reliability.