



Riverside City College Academic Senate

Agenda

Monday, 21 April 2025 • 3:00 - 5:00 PM

Meeting Location: The RCC Hall of Fame Room

YouTube link for viewing:

<https://www.youtube.com/channel/UC9tCDF4RDXCqzrUS0QfO09A/featured>

- 3:00 I. **Call to Order**
- 3:05 II. **Approval of the Agenda**
- 3:05 III. **Approval of the Minutes** Tabled for May 5
- 3:05 IV. **Public Comments**
- 3:15 V. **Liaison Reports**
- A. RCCD Faculty Association
 - B. College President or designee
 - C. ASRCC Representative
- 3:30 VI. **Committee or Council Updates and Reports**
- 3:30 VII. **Ongoing Business**
- A. President Scott-Coe or designee will distribute the Security Audit Report for Senate review in advance of VP Business Services Kristi DiMemmo’s safety and facilities update to RCCAS on May 5 (information)
 - B. President Scott-Coe will review ongoing suggested clarification edits to the RCCAS bylaws with proposed timeline for approving these updates and any other adjustments this academic year (first read)
 - C. President Scott-Coe, VP Taylor, and Secretary-Treasurer Bottoms will facilitate continued Senate discussion of the ASCCC Position Paper, “Protecting the Future of Academic Freedom During a Time of Significant Change,” with a focus on the distinction between freedom of speech and academic freedom, and brainstorming practical, proactive faculty steps to address misinformation (discussion)
- 3:55 VIII. **New Business**
- A. VP Taylor will preview resolutions for ASCCC Spring Plenary and remind departments about our process for gathering feedback on items as needed from division, department, and/or discipline experts (information + discussion)
 - B. VP Taylor or designee(s) will provide information about hosted webinars April 21-24 for Black Student Success Week as well as an update about new Umoja evening counseling hours (information)
 - C. Ratification of new and ongoing appointments: President Scott-Coe or designee will present candidates (action)
 - a. Final faculty nominees for ASCCC CCN Convenings in June
 - b. Senate representative for spring commencement committee (Secretary-Treasurer Megan Bottoms)
 - c. Faculty Co-Chair for SAS
- 4:25 IX. **Officer Reports**
- A. Vice President
 - B. Secretary
 - C. President
- 4:35 X. **Open Hearing**
- 4:55 XI. **Learn, Share, Do**
- 5:00 XII. **Adjourn**

Next RCCAS Meeting: Monday 5 May 2025

Agenda items due by Tuesday 29 April 2025 at noon

Title 5 §53200 and RCCD Board Policy 2005

Academic Senate “10+1” Purview Areas

1. Curriculum, including establishing prerequisites and placing courses within disciplines* 2. Degree and certificate requirements* 3. Grading policies* 4. Educational program development* 5. Standards or policies regarding student preparation and success* 6. District and college governance structures, as related to faculty roles** 7. Faculty roles and involvement in accreditation processes, including self-study and annual reports** 8. Policies for faculty professional development activities* 9. Processes for program review** 10. Processes for institutional planning and budget development** 11. Other academic and professional matters as mutually agreed upon between the governing board and the Academic Senate**

* The RCCD Board of Trustees relies primarily on the recommendations of the Academic Senate

**The RCCD Board of Trustees relies on recommendations that are the result of mutual agreement between the Trustees and the Academic Senate

Consistent with Executive Order N-29-20 and Government Code sections 54953.2, 54954.1, 54954.2, and 54957.5, the Riverside City College Academic Senate will swiftly provide to individuals with disabilities reasonable modification or accommodation including an alternate, accessible version of all meeting materials. To request an accommodation, please contact Office of Diversity, Equity, & Compliance at 951-222-8039.

FINAL REPORT

Districtwide Security Assessment Services, RFQ/P No. 1823/241

Riverside Community College District

Project ID: D24065
December 20, 2024



Prepared By

Nick Heywood
AVP Low Voltage Systems
DPB Engineering, Inc dba Salas O'Brien
Engineers, Inc
150 El Camino Real
Tustin, CA 92780
669.252.3621
nick.heywood@salasobrien.com

Prepared For

Beiwei Tu, EdD, ARM, CIH, CSP
Director of Risk Management
Riverside Community College District
3801 Market Street,
Riverside, CA 92501
951-222-8128
beiwei.tu@rccd.edu



CONTENTS

Executive Summary.....	4
Background and Project Approach	5
Methodology.....	7
Approach	7
Department of Homeland Security Best Practices for Anti-Terrorism Security (BPATS) for Commercial Facilities ...	8
Individual Findings Risk Prioritization	9
Crime Prevention Through Environmental Design (CPTED).....	10
CAP Index Analysis	12
Stakeholder Perspective	17
Perceptions Survey.....	18
Students	18
Employees	18
District Level Physical Security Findings.....	20
Physical Security Mechanical	20
Security Electronics Technology	23
Exterior Lighting Evaluation	27
Policy and Procedure Review.....	36
The Future	42
Roadmap	42
Identity, Leadership and Ownership.....	43
Systems Unification or Integration	43
Systems Governance.....	45



Systems Maintenance and Performance Checks	46
Division 28 Standards.....	46
Appendix A – Stakeholder Perspective (In-Depth Notes)	48
Appendix B – Perceptions Survey (Students and Employees)	54
Appendix C - District Level Physical Security Findings	66
Appendix D – High-Level Exterior Lighting Assessments	155
Appendix E – Crimecast CAP (Crimes Against Persons and Property) Index Reports.....	156
Appendix F - College Campus and District Buildings Observation and Recommendations Reports	157



Executive Summary

This assessment evaluates the current safety and security measures across Riverside Community College District (RCCD) campuses and facilities to establish a baseline for improvement. The focus is on enhancing security systems, addressing vulnerabilities, and creating standardized safety culture district wide.

The evaluation revealed several strengths, including localized safety measures and stakeholder commitment, alongside opportunities for improvement. A lack of unified management for the security program was identified as a critical barrier to standardization. Outdated and non-integrated security technologies, such as video surveillance and access control systems, reduce operational efficiency. In addition, inconsistent application of security protocols and inadequate training across campuses were noted as key vulnerabilities.

Key risks were identified and prioritized based on their impact and urgency. High-priority issues include the modernization of security electronics and the implementation of robust emergency communication systems. Medium-priority concerns involve enhancing training programs, while low-priority risks focus on improving wayfinding and standardizing signage.

The report recommends establishing a centralized approach to overseeing and standardizing policies to address these challenges. It also highlights the need for a transition to unified, integrated security technologies, such as updated video surveillance and access control systems. Additionally, mandatory emergency preparedness and response training for all personnel is essential, alongside infrastructure improvements.

Strategically addressing these vulnerabilities will create a districtwide culture of safety and security, improve operational efficiency by unifying security technologies, and enhance perceptions of safety for students, staff, and the community. Implementing these recommendations through a phased approach will strengthen RCCD's security posture and demonstrate the leadership's commitment to safety. This effort will mitigate risks, reduce liability, and foster a secure, welcoming environment for learning and employment.'



Background and Project Approach

The purpose of this report is to provide RCCD with an impartial third-party evaluation of its current security operations and insights into stakeholder perspectives on safety and security. This will help RCCD to develop a security program improvement plan.

Riverside Community College District (RCCD) has assigned Salas O'Brien Engineers, Inc. and Aanko Technologies (SOBE/Aanko) to conduct a comprehensive physical security program review of all District campuses to establish a baseline status that can be used as a foundation to develop, grow, and strengthen its District-wide physical security program to better protect and serve its communities. This security program review involves site visits, existing documentation evaluation and stakeholder interviews to evaluate physical components including security electronic systems, policies and procedures, socio-environmental conditions, training programs, and security staffing levels. The physical site assessments for all campuses were conducted during their typical hours of operation, before and after hours of typical operation, with the assumption that the security components and electronic systems were in good working order and functioning normally.

The assessed campuses and facilities were:

- Riverside City College (RCC)
- Moreno Valley College (MVC)
- Norco College (NC)
- Ben Clark Training Center Buildings #3 and #5
- Center for Social Justice and Civil Liberties
- Culinary Arts Academy
- District Office (DO)
- Henry W. and Alice Edna Coil School for the Arts
- Norco Innovation Center

The physical assessments provide RCCD with a comprehensive source of information that can serve as a baseline for future planned physical security enhancements. RCCD is considering a program that will upgrade the established physical security program at all campuses to ensure consistent application of the latest security measures across all RCCD learning and administration facilities.

We reviewed and analyzed the current RCCD Board, published policies and procedures relating to safety and security and provided comments and recommendations. Our evaluation of the policies and procedures was based on the best typical practices for assessing community colleges and our experience with other educational institutions with which we have partnered. All board-published policies and procedures reviewed in this document can be found at the following link:

<https://www.rccd.edu/bot/policies.html>

We also performed a wider analysis of each RCCD campus' socio-environment using Crimecast CAP (Crimes Against Persons, Crimes Against Property) Index reports. These reports provide RCCD with snapshot of crime activity based on



law enforcement crime statistics. We have provided comments on each campus' specific CAP Index report further in this document (See CAP index Analysis and Appendix C). This analysis and the crime statistics reported should be factored into the bigger picture holistic security program thought process. Reported crime activity may influence the deployment of security personnel or influence certain physical security components use, such as door hardware functionality.

This report identifies and illustrates the positive existing physical security measures deployed by RCCD across its current facilities. We also identify deficiencies, inconsistencies and areas that do not meet best practices and security device installations that do not provide the best return on investment for RCCD.

It is recommended that this report remain confidential to the RCCD and be protected for public viewing by the California Public Records Act. The California Public Records Act (CPRA) is a series of laws designed to guarantee that the public has access to public records of governmental bodies in California. Statutes 6250 - 6270 define the law. CPRA lists several exceptions to this act, specifically documents related to protecting staff, clients, and property. These documents can include assessments, design plans, training, policies, and standard operating procedures.

Section 6254, California Government Code (aa), Allows an exception from being publicly accessible for a document prepared by or for a state or local agency that assesses its vulnerability to a terrorist attack, or other criminal acts intended to disrupt the public agency's operations and that is for distribution or consideration in a closed session.



METHODOLOGY

Approach

Our approach to performing physical site assessments and reviewing policy and procedures is from an interfaced, operational, built environment, and technology perspective. Rather than focusing specifically on any one element, we identify, analyze, and recommend enhancements and considerations that will improve the security program holistically. This approach evaluates the relationships between multiple security components, such as how video surveillance deployment and video recording usage policy work together to provide a built environment supported by both technology and governance policy.

To ensure that comprehensive and cost-effective solutions are pursued, we do not simply focus on isolated elements of risk mitigation, such as the implementation of automated security systems at one location. Instead, our efforts are designed to address all the interrelated elements of a security program, including **operational issues**, such as safety and security policies and procedures, training, visitor management, lockdown, evacuation, and emergency preparedness; **electronic systems**, such as video surveillance cameras, intrusion alarms, access control, and mass communications systems; **architectural issues**, such as space planning, landscaping, safe egress routes, lighting, signage, perimeter barriers, and locks; and **environmental and workplace concerns**, such as congestion, traffic flow, adverse conditions, local community involvement, and staff and faculty perception.

We perform site assessments accompanied by users of the facility (when available) who have intimate knowledge of the sites and understand how they function from an operational perspective. Often, engaging custodians or facilities team members provide invaluable insight into back-of-house space, uncovering vulnerabilities not seen from the public side of buildings. During the assessment, facilities staff, faculty, and administration staff provide direction and access to spaces upon request. We frequently interact with campus faculty and observe campus user behavior before, during, and after hours to gain insight into how they act and behave within the campus environment and existing security measures.

We evaluate the security posture from a physical perspective using established security industry practices and a layered approach. Our assessment approach initially starts from the outside looking in, observing what is applied consistently across the campus to demonstrate a Districtwide layer and approach to security. Policy and procedures are typically captured within the Districtwide layer. The physical component perspective involves sequentially working our way from the site perimeter to the core of each campus and/or building, with focus and evaluation on property perimeter, parking lots, building perimeter, classrooms, and critical infrastructure space. Adopting a systematic and defined approach ensures uniformity of site reviews and supports the identification of consistent and/or inconsistent physical security measures across different locations.

The layered evaluation of RCCD's physical security program is illustrated in Figure 1. This approach helps us identify situations where failure to enforce a certain activity can be mitigated by employing another supporting security measure. For example, an unlocked interior classroom door can be mitigated by ensuring secured exterior building entry doors. This reduces the risk of theft if a classroom door is left unlocked overnight. This is further supported by the policy of authorized access only via authorized credentials to spaces.

The American Society for Industrial Security (ASIS) recognizes the following **5 key principles** of physical security: **Deter, Detect, Delay, Respond, and Mitigate**. We consider how the existing security measures in operation help achieve each of these principles. The individual site observations provided in Appendix A identify vulnerabilities and weaknesses that require the key principles applied to support the correction of the issue.

It is important to note that the SOBE/Aanko approach acknowledges good practices observed, in addition to remarking on program deficiencies. Communication with campus end-users during the site assessments creates dialogue and sharing of information with those intimately familiar with the day-to-day operation of the facilities. The insight obtained during the site assessments provides valuable information and an operational understanding of some excellent measures that are currently in place.

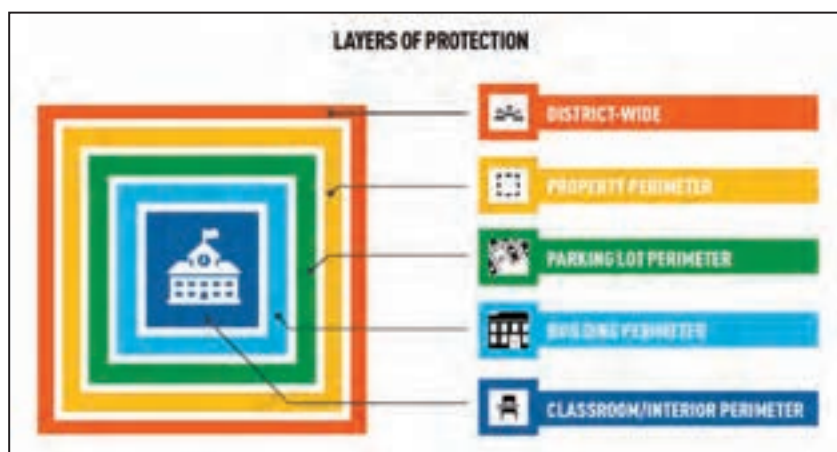


Figure 1 - PASS Layers of Protection¹

Department of Homeland Security Best Practices for Anti-Terrorism Security (BPATS) for Commercial Facilities

We utilize the Department of Homeland Security's Best Practices for Anti-Terrorism Security (BPATS) for Commercial Facilities framework², along with industry best practices, to assess the RCCD campuses and facilities. The BPATS methodology is scalable and can be customized to suit educational institutions. BPATS provides a consistent approach to security practices, with specific procedures, methods, equipment, or systems that are related to preparing for, preventing, mitigating, and recovering from acts of terrorism. These practices are applied as appropriate within the individual campus and facility recommendations found in Appendix A.

¹ <https://passk12.org/>

² <https://www.safetyact.gov/BPATS>



Individual Findings Risk Prioritization

The on-site physical assessments conducted at RCCD campuses and facilities involved assigning a prioritization level to each observation based on the level of risk posed concerning the safety and security measures observed at each location. This approach facilitates the formulation of a phased review and corrective action schedule and program that could be adopted by RCCD to support and substantiate future fiscal budgeting for corrective action by prioritization and risk levels. Additionally, general observations were made and documented as applicable. The assessments reveal that several safety and security practices are already in place and function well. These practices were acknowledged and documented accordingly. It is recommended that the RCCD consider applying practices consistently across all campuses as this will provide immediate enhancement of existing safety and security measures with no fiscal impact to the RCCD.

Each campus assessment observation has an associated table that contains a photograph of the observation, and recommendations for corrective action, recommendations are specific to the observation.

To categorize programming, scheduling, and funding of corrective actions, a point scoring system is used to assign risk prioritization and ranking to each observation that are color-coded and identified in each campus observations table. This system helps the District allocate resources and plan its budget to address the issues that present the highest risk and liability.

The risk prioritization allocation approach adopts a range of scoring from the lowest score of zero for simple observations made that present no negative impact on the safety and security program through to the highest scoring of 5. Items identified as a 5 are designated as severe prioritizations that may result in immediate risk to life or property. These risk prioritizations should be addressed immediately with mitigating action. The risk assignment levels have been established through past experiences working with clients to determine levels of risk appropriate to assignment of observations made. Based upon the district’s risk appetite the assigned risk level applications can be scaled up or down accordingly.

Risk Prioritization and Ranking Table			
Risk Prioritization	Risk Ranking	Description	Example
Severe	5	Can result in immediate risk to life or property. Corrective action is required immediately.	Emergency egress opening padlocked shut, ability to egress through defined exit point not available.
Major	4	May cause ease of breach to physical security posture or impact incident response if not addressed efficiently.	Emergency evacuation routes are not identified within the emergency operations plan. Access control openings are propped open when in a locked state.
Significant	3	Not immediately impacting the physical security posture or incident response but is lacking in performance or content and requires review.	Emergency blue tower strobe does not activate when a call is placed. Call pick-up occurs after roll-over from one dispatch phone to another.



Minor	2	No significant impact on the security program but awareness and a plan to mitigate are suggested as to avoid escalation of risk ranking.	Door astragal is weather damaged and provides visibility in from the exterior side, door's secure state is not compromised.
Insignificant	1	Minor issue with no significant impact on security measures. Provided for visibility and future corrective action if necessary.	Video surveillance camera protective lens cover requires cleaning to maintain a clear field of view.
Observation	0	No negative risk associated may be a positive that promotes ease of measure adoption across other facilities.	Main administration office is identified with signage providing directions for visitors to sign in upon arrival.

Table 1 - Risk Prioritization

Crime Prevention Through Environmental Design (CPTED)

CPTED is a multi-disciplinary approach of crime prevention that uses urban and architectural design and the management of built and natural environments. CPTED strategies aim to reduce victimization, deter offender decisions that precede criminal acts, and build a sense of community among inhabitants so they can gain territorial control of areas, reduce crime, and minimize fear of crime. CPTED supports cost effective environmental security review, promotes community buy-in, and environmentally sustainable solutions identification that when deployed can provide benefit to a security program. The four principles of CPTED are:

Natural Surveillance

We assess campus facilities through the lens of providing natural surveillance capabilities, maintaining clear lines of sight, and identifying areas where lack of visibility may provide opportunity for persons with bad intent to hide or obscure themselves from visibility. Windows, lighting, and removal of obstructions can be placed to improve lines of sight from within buildings.

Natural Access Control

Review of access control measures such as placement of doors, perimeter fences, shrubs, trees, and other physical components that can be used to provide natural access control measures. Fundamentally, the intent is to keep unauthorized persons from areas where they have no legitimate reason for being there. We review natural paths of egress etc. as part of this approach ensuring that attempts to provide natural access control measures do not impede evacuation routes and egress.

Territorial Reinforcement

Observation of boundaries clearly defined by signage, well maintained landscaping and building material. That provide insight into how territorial reinforcement between public and private spaces is achieved. We observe campuses to determine if simple measures such as colored paving is used to separate areas of safe pedestrian access from vehicle entry points etc. is in use.

Maintenance and Management

Effectiveness of CPTED measures are often impacted if maintenance and management of measures does not occur. For example, well defined access control measures impacted by graffiti on a building or wall that is not removed in a timely manner, can provide a negative impact that “no-one” cares about the big security picture and the good measures in place are not respected by facility users. Maintenance activity such as landscape management is critical to maintaining the effectiveness of the intent of deployment to support a security posture.

We use the CPTED principles to designate, define and design spaces that provide long-term security sustainability to campus facilities.

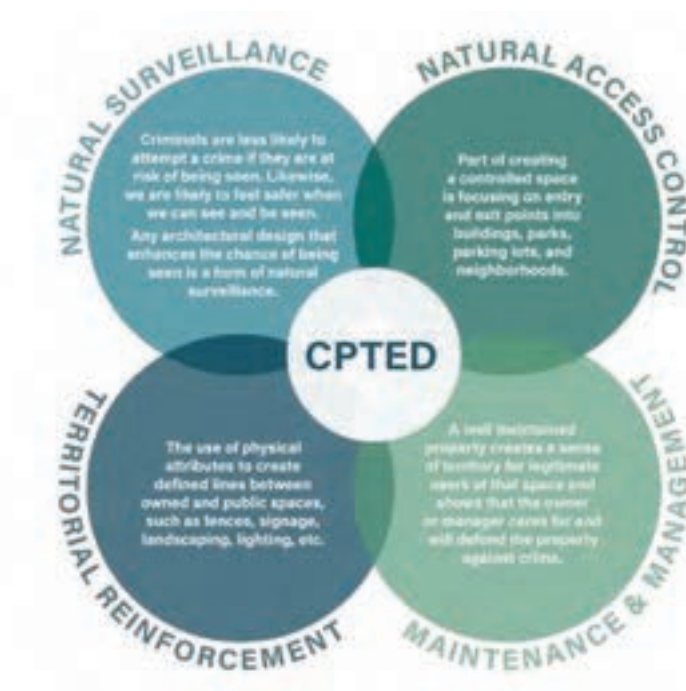


Figure 2 - CPTED Principles

During the on-site assessment, we consider the surrounding community and environment for their impact on the buildings/sites reviewed. Our team conducts a comprehensive review of the perimeter, points of entry and exit to the facility, paths of travel for both vehicles and pedestrians, and overall compartmentalization of the buildings and sites. We also review site lighting during hours of darkness and identify areas for improvement in the overall site lighting strategy.



CAP Index Analysis

SOBE/Aanko conducted an analysis of local crime statistics and the threats facing the RCCD campuses and administrative facilities based on CRIMECAST reports produced by CAP Index. The CRIMECAST scoring model includes analysis of neighborhood demographics (excluding race, religion, and other protected categories), national police data, local police data, client loss reports, offender surveys, victim surveys, education data, economic data, and other databases with known indicators of crime. Their method is based on the strong relationship between a neighborhood's "social disorganization" and the amount of crime that occurs there. Social disorganization theory is intricately linked to the "ecological perspective" of crime, delinquency, and human behavior, which views criminal activity as the product of weakly-organized social environments. Some of the kinds of demographic predictors used in their model include population and housing distributions, age distributions, housing values, family and household membership, marital status, home ownership, number of vehicles, income amounts and sources, educational levels, and employment rates. The data is then structured around seven types of criminal activity recognized in the tradition of common law. Four classifications of crime are directed towards individuals (i.e., homicide, rape, robbery, and aggravated assault), and three categories of crime targeting property (i.e., burglary, larceny, and motor vehicle theft). Utilizing these categories and relying upon demographic variables, historical crime data, survey information and other known indicators of crime, it is possible to organize crime rates based on specific neighborhoods to then be used in an analysis such as what was conducted for RCCD.

CRIMECAST scores are based on a scale from 0 to 2000, with 0 being the lowest risk, 2000 the highest risk, and 100 representing the national average risk. A score of 50 represents half the risk of the national average, while a score of 200 represents double the risk of the national average.

Three individual reports were created that captured all facilities within scope, a 3-mile radius parameter was set for both NC and RCC based on proximity of associated facilities in scope. A six-mile radius was set for MVC, capturing the Ben Clark Training Center buildings.

The statistics generated by the CRIMECAST reports identified that NC is located within the area with the highest CAP Index score of the three campuses. NC scored 261 which is 2.6 times the national average from a risk perspective. RCC and MVC recorded scores of 229 and 202 respectively, see Table 2. Simply reviewing the scores alone does not provide a true reflection on the individual locations and crime that may or may not occur. The mapping provided in Figures 3, 4, and 5 illustrates the wider environment within the parameter of the crime statistic reach. This is important to provide context and understanding of how CAP Index scores are generated and reflect how specific areas and pockets of areas in the locality can have significant impact upon a generated score. For example, it is evident that although NC recorded the highest score of 261, the areas of high crime activity are restricted to certain areas shown in red on the map provided in Figure 3. The area specifically adjacent to the north of the college campus, and north and south of CA-91 have scores of 335, 392, 409, and 486, in contrast to areas close to the college immediate vicinity beyond the Naval Base that score below 50 extensively. The report is generating the CAP Index score based on the average of all of these locations and the map supports understanding of criminal activity within the wider geographical range, which may not be a direct reflection on the campus location itself. The potential threat, risk, and impact of high crime activity in the wider geographical location should be considered as potential influences on how security measures are deployed at the NC campus.



The map in Figure 4 clearly illustrates that the areas immediately north and to the east of the RCC Campus significantly impact the overall score (229) associated with the campus. Several pockets of the adjacent downtown area experience six-times the national average crime activity with burglary and motor vehicle theft frequently occurring. The higher crime scoring within a downtown area is typical and reflects the higher population density often found due to daily influx of commuters and visitors who inflate statistics as a downtown area may only have 10,000 residents but a daily population of 100,000 workers. Interestingly despite being an area of high population the homicide rate recorded at the RCC campus was the lowest recorded of the three campuses. The CAP Index score specific to the locale of the campus is 17 clearly representing that the crime that occurs (and is reported) at campus is below national average scores. It is important to consider the CAP Index crime activity as immediately adjacent to the campus the score is above 300, and criminal activity can easily creep into the campus if appropriate deterrent and detection measures are not deployed.

MVC campus recorded the lowest score (202) with this score impacted by a further out-reach of 6-miles to encompass the Ben Clark Training Center. The map in Figure 5, illustrates the areas of higher crime rates with one pocket recording above 600. The areas in the immediate locale score in most cases well below 100. The geographic location of the campus also contributes significantly to the lower crime activity with the campus adjacent to recreation areas and on the periphery of the city which has a population upwards of 205,000.

The District Office, Henry W. Coil Sr. and Alice Edna Coil School for the Arts Center, Center for Social Justice and Civil Liberties, and Culinary Arts Academy Restaurant are all located within the downtown Riverside 3800 and 3900 blocks. These facilities are located in a 500+ scoring area. This reflects the lack of sense of safety and security by facility users as openly expressed in interviews and through verbal discussion and visual observation. These building locations present areas of interaction with homeless and agitated persons on a frequent basis in this two-block area, providing a heightened sense of concern regarding safety and security which is not experienced at the college campuses. The crime statistics alone illustrate that increased security measures both physical and staffing require a more robust approach and consideration in relation to the individual campus approaches. Consistence of security measures application across these facilities should be a main priority, ensuring that no one space has less security than another.

As stated herein, statistical analysis alone of reported crime should not singularly drive future safety and security measures. Review, acknowledgement, and consideration of reported crime along with reported crime at each campus and facility via the regulatory annual Clery Act reporting, should all be factors and information providers that are considered. Additionally, perception survey and interview findings will further provide context to campus and facility users overall perspective on safety and security across RCCD.



	Norco College	Riverside City College	Moreno Valley College
CAP INDEX® SCORE	261	229	202
CRIMES AGAINST PERSONS	437	257	241
Homicide	408	184	206
Rape	262	231	218
Robbery	258	249	200
Aggravated Assault	562	275	264
CRIMES AGAINST PROPERTY	295	380	236
Burglary	274	408	225
Larceny	276	357	219
Motor Vehicle Theft	440	460	419
SUPPLEMENTAL SCORES			
Simple Assault	418	233	265
Vandalism	317	294	232

Table 2 - Riverside Community College District Campus CAP Index Scores



Figure 3 - NC CAP Index Mapping



Figure 4 - RCC CAP Index Mapping



Figure 5 - MVC CAP Index Mapping



GEOGRAPHIC LEVEL	UNITED STATES			CALIFORNIA			RIVERSIDE COUNTY		
	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029
CAP IndexSM Score	265	261	259	223	217	219	250	239	244
CRIMES AGAINST PERSONS	457	437	423	390	378	373	371	349	349
Homicide	449	408	418	502	454	471	434	396	424
Rape	329	262	256	237	213	267	196	214	212
Robbery	279	258	258	218	200	207	261	243	250
Aggravated Assault	481	502	541	512	498	484	448	417	416
CRIMES AGAINST PROPERTY	267	290	382	315	233	233	247	285	281
Burglary	369	374	371	317	228	243	309	267	277
Larceny	338	376	260	322	266	258	364	397	296
Motor Vehicle Theft	541	480	423	288	238	242	316	265	267
SUPPLEMENTAL SCORES									
Simple Assault	409	418	401	453	466	458	363	357	351
Vandalism	325	317	305	363	362	380	325	359	315

Table 3 - Country, State, County CAP Index Overview – PAST, CURRENT, PROJECTED

RCCD facilities assessed all fall within Riverside County, CA. A holistic overview of past, current, and future reported crime is detailed in Table 3. Current criminal activity reported places Riverside County below reported crime in most crime types, but above state reported activity specifically in crimes against property. The future projected crime level increases with an overall increase in forecast crimes against persons (potentially due to expected population increase) and a small reduction in crime against property. The big picture outlook is that Riverside County will remain below the projected CAP Index scores assigned to the United States collectively but will remain slightly above state projections.



Stakeholder Perspective

The inclusion of diverse stakeholder perspectives is essential for enhancing safety and security across RCCD campuses. Interviews with more than 60 key stakeholders including faculty (24), classified employees (11), and administrators (26) highlighted various challenges and opportunities related to campus safety, emergency preparedness, and public safety infrastructure, revealing key themes:

1. **Campus Security Presence:** Stakeholders expressed concerns about the visibility and effectiveness of campus police, particularly during nighttime and in secluded areas. A reduction in proactive engagement has increased feelings of vulnerability. Many noted high turnover rates and leadership instability within the police department, leading to inconsistent response times and a breakdown of trust.
2. **Communication Deficiencies:** Participants reported significant gaps in communication regarding security incidents. Many felt that important information was poorly conveyed or lacked timely updates, contributing to anxiety and confusion during emergencies.
3. **Physical Security Infrastructure:** Numerous concerns were raised about inadequate physical security, including malfunctioning surveillance cameras, poor lighting, and outdated access control systems. Participants advocated for improvements in security infrastructure to mitigate vulnerabilities.
4. **Emergency Preparedness:** There was a consensus on the need for comprehensive safety training across campuses. Many faculty and staff felt unprepared for various emergencies, emphasizing the importance of regular drills and clear leadership roles during incidents.
5. **Student Mental Health:** Concerns regarding the mental health of students were prevalent, particularly post-COVID-19. Many emphasized the need for better coordination between mental health services and campus safety to address potential crises effectively.

Recommendations for Improvement:

- **Mandatory Safety Training:** Implement regular emergency response training for all personnel.
- **Increased Public Safety Presence:** Enhance police visibility, especially during evenings.
- **Improved Communication Protocols:** Develop structured communication systems for reporting incidents.
- **Upgraded Security Infrastructure:** Invest in better physical security measures, such as key card systems and enhanced lighting.
- **Expansion of Mental Health Services:** Increase mental health resources and training for faculty to manage student crises effectively.



Perceptions Survey

In addition to the stakeholder interview, a district-wide perceptions survey was conducted engaging faculty, staff, and students. The perceptions survey support generation of engagement on a large-scale and allowed for completion using both thin or thick clients and mobile devices. Microsoft Forms was utilized to present the survey with all responses anonymously provided with opportunity for respondents if they chose to provide contact information for further follow-up at their discretion.

As with stakeholder interviews, the survey promotes inclusivity of an extensive range of campus end-users whose perception, visibility, and use of campus facilities provides invaluable insight that third-party assessors are unaware of from a day-to-day operations basis.

The districtwide perception survey engaged faculty, staff, and students to gather insights on safety and security across Riverside Community College District (RCCD) campuses. Over two weeks, the survey collected 485 responses, revealing key concerns, strengths, and areas for improvement from diverse stakeholders.

Students

Survey responses included two hundred thirty-six (236) participants, with an average completion time of thirty-two (32) minutes. RCC students were the most engaged, contributing 151 responses. Students expressed concerns about the open-campus design, minimal police presence, and the lack of visible and functioning security technologies, such as surveillance cameras and lighting in parking areas. They also highlighted issues with communication during emergencies, unsafe interactions with transients, and inadequate mental health resources. Many students reported limited familiarity with emergency procedures and a lack of engagement in safety-related training or drills. Recommendations included increased campus police presence, improved lighting, enhanced access controls, and more effective communication systems.

Employees

Employees shared similar concerns, particularly about minimal police presence and outdated security technologies. They emphasized the challenges posed by communication delays with offsite dispatch and the limited ability to secure classrooms during emergencies. Employees noted that emergency procedures were inconsistently implemented, and training participation was low. Some advocated for improved infrastructure, such as panic buttons in classrooms and restricted building access.

Shared Concerns and Opportunities

Both students and employees emphasized the importance of visible campus police patrols, particularly at night, and functional security technologies. The perception of nonoperational cameras and emergency call stations was a recurring theme, suggesting an urgent need for system audits and upgrades. Both groups also highlighted the lack of consistent communication during emergencies, with calls for clearer incident updates.



Despite shared concerns, the survey revealed varying levels of engagement with existing safety measures. While students were more vocal about the need for a stronger campus police presence and visible security measures, employees focused on practical tools like phones, protocols, and drills to enhance response capabilities. Both groups acknowledged some strengths, such as existing communication systems and the commitment of campus police; these strengths were overshadowed by concerns about response times and outdated systems. Stakeholders across both groups stressed the importance of standardized protocols, regular training, and visible safety measures to create a secure learning and working environment.



District Level Physical Security Findings

Physical security within education institutions is intended to provide a safe and secure learning and working environment for students, faculty, staff, and visitors. Within this section we detail the observation findings of the physical assessments and provide recommendations and suggestions for district level enhancement. The findings provided summarize observations across the district facilities for both physical components and security technology applications.

PHYSICAL SECURITY MECHANICAL

SECURITY MEASURE	OBSERVATIONS	RECOMMENDATIONS
Brass Keys	<ul style="list-style-type: none"> No centralized key management approach Issuance and retrieval process varies by campus Lack of Board Policy addressing non-return of keys consequence Restricted keyways are used across all campuses Unaccounted for keys 	<ul style="list-style-type: none"> Standardize on a single district keyway Implement a single process for key issuance and retrieval Maintain key records using key control software Create Board Policy that mandates key management process, expectations, and consequence of non-compliance
Door Hardware	<ul style="list-style-type: none"> Lack of District standard for Division 08, several different hardware manufacturer products installed Hardware functionality installation lacks consistency of application based on space function Inadequate hardware functionality applied to spaces occupied by students and faculty Disparate operational expectations of door hardware use across campuses Lack of end user knowledge of door hardware function 	<ul style="list-style-type: none"> Create Division 08 door hardware standards, simplify product procurement and apply appropriate hardware based on space usage and occupation Apply Lock Bloks in a consistent manner, do not leave areas vulnerable to breach and immediate door securing ability Remove ability to “dog” electrified panic bars Implement operational expectation of door status and enforce consequences for non-compliance
Glazing and Door Treatments	<ul style="list-style-type: none"> Existing film is not ballistic preventative 	<ul style="list-style-type: none"> Evaluate known areas of vulnerability and exposure to anti-



SECURITY MEASURE	OBSERVATIONS	RECOMMENDATIONS
	<ul style="list-style-type: none">▪ Large areas of exposure through non-tinted glazing from the exterior side▪ Existing film requires maintenance repair/replacement as peeling providing vulnerability to interior occupants▪ Inconsistent application of window treatments and operational use▪ Floor to ceiling glazing without additional barrier protection at Downtown Riverside locations	<p>social public activity for addition of ballistic and restrictive visibility film</p> <ul style="list-style-type: none">▪ Apply standard window treatment applications to areas of similar space usage, promote consistency of application type i.e., shades and blinds▪ Engage law enforcement and first responders to gather their perspective and needs for visibility into buildings during an incident response
Vehicle Controls and Perimeter Protection	<ul style="list-style-type: none">▪ Existing vehicle barriers are not utilized to restrict vehicle access onto campuses▪ Existing garages have access vulnerabilities with unenclosed first floor accessibility▪ Speed restrictive measures i.e., speed bumps and raised crosswalks are minimal and fail to reduce vehicles speeds across campuses▪ Mobile signage is easily moved and negated in its intent▪ Lack of delineation of vehicle access points and permitted speed	<ul style="list-style-type: none">▪ Apply speed cushions and speed bumps to reduce vehicle speeds and not compromise first responder response▪ Replace mobile signage with fixed▪ Review operational intent of existing swing-arm barriers, determine if they should be used on a daily basis to reduce vehicle access outside typical hours of operation▪ Reinforce vehicle lanes with pavement markings▪ Install speed limit signage consistently across all campuses
Fencing and Gates	<ul style="list-style-type: none">▪ Areas of vulnerability with existing fence heights failing to restrict visibility into facility space i.e., Early Education Centers▪ Various states of disrepair of existing fencing▪ Existing gates unlocked at areas that signage indicates authorized access required	<ul style="list-style-type: none">▪ Create a minimum standard for fencing height, type, material based on application needs▪ Define a minimum height for fencing, 8' minimum recommended, 10' preferred▪ Perform maintenance repair and replacement of existing damaged fencing



SECURITY MEASURE	OBSERVATIONS	RECOMMENDATIONS
	<ul style="list-style-type: none">▪ Neighboring properties have unrestricted campus accessibility through site adjoining gates▪ Landscaping overgrowth causing damage to existing chain link fencing	<ul style="list-style-type: none">▪ Deploy appropriate fencing based on application and placement needs, consider decorative fencing and toppers where appropriate
Signage and Wayfinding	<ul style="list-style-type: none">▪ Wayfinding maps and signage are sparse and, in several locations, require update to reflect current campus layout▪ Signage is impacted by sun-bleaching with the ink faded and information illegible▪ Door numbering and signage appearance varies across district facilities, no standardized approach▪ Emergency call stations lack identification through physical signage▪ Excellent use of photoluminescence emergency evacuation plans at Norco College▪ Digital maps online not accessible	<ul style="list-style-type: none">▪ Refresh all existing wayfinding with current campus layouts, add additional wayfinding maps▪ Review the online web maps and ensure no issues with the links when accessed remotely▪ Adopt a consistent appearance for all campuses that reflects the RCCD image/colors, campus users should know they are on an RCD campus/site▪ Implement photoluminescence emergency evacuation plans at all locations▪ Implement a standard text, size and color of all fonts used for building and door numbering▪ Consider rooftop building identification for air responders

Table 4 – Physical Security Observations and Recommendations



SECURITY ELECTRONICS TECHNOLOGY

SECURITY MEASURE	OBSERVATIONS	RECOMMENDATIONS
Access Control	<ul style="list-style-type: none">Existing system is CCure 9000 with no integration with other systems i.e., video surveillance (minor integration with intrusion). System is using older hardware that is not reflective of current technology and hardware that is supported by the manufacturer.Disparate versions of software in operation across RCCD campuses fail to offer all campuses same systems capabilitiesSoftware Support Agreements (SSAs) are not consistent with different levels of service provided by support vendorsNo proactive use of access control to actively manage the RCCD security posture, no systems oversight or management from a district levelLockdown capability is applied to some buildings with access control deployedCredentials are 13.56 MHz high encryption; some credentials have end user photo applied	<ul style="list-style-type: none">Perform a systems comparison evaluation of the existing system versus others to determine if the existing system or other is most appropriate for RCCD operational needsAnalyze a migration plan of upgrading the existing system hardware if CCure 9000 identified as the system for the futureDevelop Division 28 security electronics standards to cover approved systems use, edge devices, and placement of devices for all systemsHardwire all lockdown and duress buttons for supervision of button status, evaluate the risk of campuses with hybrid of lockdown buttons and buildings with no access control to support lockdown capabilityApply photo identification to all security credentials issued to staff and faculty
Intrusion Detection	<ul style="list-style-type: none">Several different systems in use, monitored off-site by third-party monitoring companyUse of card readers at some locations with Software House devices supporting audit of system useTraditional arming stations use a manual code for system arming and disarming	<ul style="list-style-type: none">Standardize the approach to application of intrusion detection, integrate with other systems for greater operational benefitMonitor all exterior openings and high-risk spaces with door position contactsPerform regular system testing to verify that systems



SECURITY MEASURE	OBSERVATIONS	RECOMMENDATIONS
	<ul style="list-style-type: none">▪ Inconsistent application of devices i.e., motion sensors and door contacts▪ Non-operational Bosch arming stations	<p>communication to the off-site monitoring station is active</p> <ul style="list-style-type: none">▪ Transition communication to cellular network reducing the cost of POTS lines
Video Surveillance	<ul style="list-style-type: none">▪ Identified more than eight (8) different camera manufacturer devices observed installed, some are no longer supported by the manufacturers▪ No centralized management of the system, old technology is in use▪ No defined minimum days of video retention (assumed 30 days), no video usage policy and a lack of systems governance▪ Video is not integrated with any other security electronics system▪ Video is not used for proactive management of RCCD facilities▪ Several standalone video management systems are in use across the district, deployed by local departments with no visibility by the district▪ Norco Innovation Center system is managed by the tenant and not the district	<ul style="list-style-type: none">▪ Standardize on security video surveillance application across all RCCD locations, system type and general camera placement creating baseline expectations▪ Ensure system compatibility and integration with other electronic security components, including intrusion detection and access control▪ Establish minimum equipment standards. such as camera types and characteristics▪ Develop a comprehensive and future-oriented plan to steer upgrades and expansions▪ Review the Norco Innovation Center video system and remove tenant access video of areas that they do not occupy▪ Consider central management of the system at a Security Operations Center (SOC) and use analytics to support camera call-up and proactive management of safety and security with video support
Visitor Management	<ul style="list-style-type: none">▪ Visitor management is limited in its application to verifying who is requesting entry to the Early Childhood Education Centers. Verification of identity is not requested at any other locations	<ul style="list-style-type: none">▪ Implement a district level policy regarding management of visitors, define the expectations of both visitors and staff and faculty when receiving guests▪ Evaluate the cost implication of using the existing access control



SECURITY MEASURE	OBSERVATIONS	RECOMMENDATIONS
	<ul style="list-style-type: none">Existing operation is typical of other community college districts with challenges implementing visitor management at open campusesDistrict Office visitors are met by the person they are visiting at the main lobby reception areaNo district visitor management policy in place	<p>system CCure 9000 “bolt-on” visitor management module</p> <ul style="list-style-type: none">Provide training and communicate to staff and faculty operational protocols for receiving and managing visitor appointmentsEncourage identification checks of persons requesting entry to buildings at the reception areas when they are unknown
Emergency Telephones	<ul style="list-style-type: none">Disparate form-factors of emergency call stations deployed across RCCD campusesMany devices are end-of-life, non-operational and present significant liability riskNo integration with video surveillance for visibility of call-up locationIncorrect form factors installed presenting issue with ADA protrusion regulationsInconsistent application of associated blue strobes, many strobes lack power and serve no purpose regarding identification of call stationsLack of instructions on use and where the call when placed will be answered	<ul style="list-style-type: none">Standardize on one product manufacturer and select typical form factors for wall mount and tower type call stationsPerform immediate corrective measures or removal of faulty unitsIntegrate call stations with video surveillance to provide visibility of the immediate vicinity when calls are activatedEnsure that blue strobes are always illuminated and strobe when calls are placedProvide information on use and the response protocol online for student and campus users to familiarize themselves with the process when a call is activated
Communication Tools	<ul style="list-style-type: none">Provision of Public Address (PA) is restricted to MVC Dental Center and Norco College onlyNo internal PA amongst any other areas across RCCD facilitiesTwo-way radios are prominent for communication purposes across all locations, the district do not	<ul style="list-style-type: none">Consider deployment of an enterprise PA system that provides immediate communication both internally and externally as required. Ability for two-way open communication path would further support the PA to be used as an overhead intercom. A PA would mitigate risk



SECURITY MEASURE	OBSERVATIONS	RECOMMENDATIONS
	<p>provide all, some are procured from big box stores by staff</p> <ul style="list-style-type: none">▪ Telephones are not installed across all RCC campus classrooms, staff and faculty cell phones are the prominent tool for communication▪ The RAVE mobile application is used by the district for distributing mass communication notifications. It is assumed that all staff, faculty, and enrolled students receive communications when enrolled on the system▪ Staff, faculty, and students advised that they often receive communications after the event, confirmation of incident resolution is not received as commonly as the initial incident alert	<p>of staff, faculty, and students not being aware of alerts if phones are silenced and placed within bags during class</p> <ul style="list-style-type: none">▪ Reinstall telephones into classrooms to provide staff and faculty with a district provided means of communication. The employee survey identified significant request for provision of telephones▪ Conduct regular validation testing so that those presumed to be enrolled in the RAVE system can be verified. Assumption that alerts are being received should be avoided as survey findings identified issues with alerts being received. Improve communication and awareness of the application, again, the survey identified several respondents unaware of its availability▪ Review the workflow of issuance of incident notification and resolution. It is important to keep campus and facility users up to date on incident activity and progress to avoid unintentional early departure or prolonged sheltering-in-place

Table 5 – Security Electronics Observations and Recommendations



Exterior Lighting Evaluation

Exterior lighting is a key component of the security measures in place and is a supplementary element that supports CPTED strategies. Proper consideration of lighting design and implementation can provide benefit to district campuses and facilities in several ways:

1. Illumination of Dark Areas

- a. Adequate lighting helps to eliminate dark areas and shadows that provide areas of hiding for criminal activity to occur.
- b. Well-lit pathways, parking lots, and public spaces enhance visibility, making it harder for criminals to hide.

2. Creating Natural Surveillance

- a. Properly placed lighting encourages natural surveillance by campus and facility users, surrounding communities, and security personnel.
- b. Natural surveillance and well-lit space allow people to clearly identify suspicious behavior and report it to appropriate security and law enforcement agencies.

3. Perception of Safety

- a. Well designed, appropriately placed, and correct application of lighting luminaires contributes to a sense of safety and security.
- b. Well-lit areas make people feel more comfortable and confident, reducing fear of crime and encouraging use of facilities providing eyes-on of activity.

Exterior lighting should be provided throughout the campuses, with special emphasis on lighting at building points of entry and perimeter illumination. Lighting can function as a physical and psychological deterrent, and it is cost-effective to maintain. Lighting is especially important for sensitive areas on a property, such as pedestrian walkways, main building entrances, parking lots, and loading bays.

We assessed the exterior lighting of each campus by using a light meter and specific lighting parameters. We illustrated the lighting levels on campus maps using a color legend. Our main method of recording the lighting levels was by using foot-candle measurements. A foot-candle is the amount of illumination that the inside surface of a one-foot-radius sphere would receive if there were a uniform point source of one candle in the exact center of the sphere. Alternatively, it can be defined as the illuminance on a one-square foot surface on which there is a uniformly distributed flux of one lumen.

Here is a straightforward illustration designed to facilitate comprehension of the foot-candle measurement. Imagine setting a candle at a distance of 0.30 meters (1 foot) from a flat wall on which we have drawn a square shape measuring 0.09 square meters (1 square foot). One lumen per square foot will illuminate this surface.

Foot-candle is the most widespread lighting measurement in the industry. Why do we still use the word “candle” to measure light in this day and age? The explanation for this choice dates back to the origins of the candle itself. When

people began to measure the intensity of light, candles were the most common light source available.³

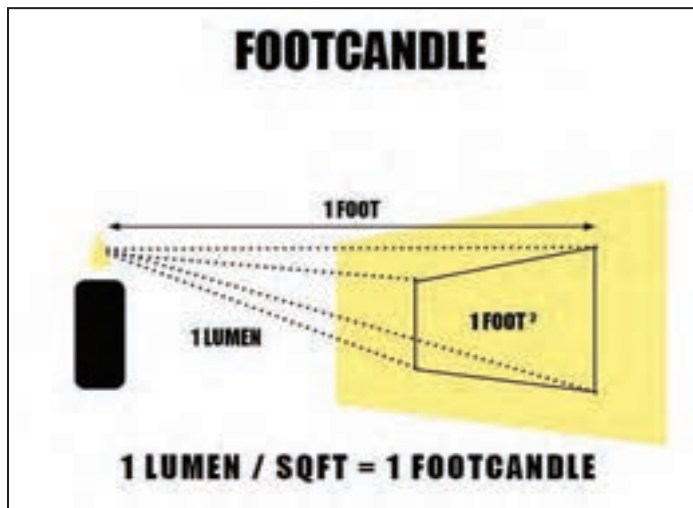


Figure 6 - Foot-candle to Lumen Diagram

Exterior lighting levels were recorded per each campus and facility and are provided in Appendix B. Each measurement recorded is color coded using the colors identified in Table 6. It should be noted that the lighting assessment performed is high level and further comprehensive detail of existing lighting levels would require a lighting consultant to be engaged. The light levels documented provide an overview of the current lighting at RCCD locations and identify areas of lighting ranging from very poor to excellent in an easy to distinguish format.

Color	Foot-Candle (FC) Level	Assessment Assigned Rating
GREY	< 0.50	Very Poor
ORANGE	0.51 – 1.02	Poor
YELLOW	1.03 – 2.32	Good
WHITE	2.32+	Excellent

Table 6 - Lighting Assessment Foot-Candle (FC) Scale

Campus Lighting Observations

Lighting findings varied across each campus with some areas under construction (i.e., parking lots at RCC and MVC) resulting in the lighting being turned off or demolished at the time of assessment. Lighting was observed as lacking power resulting in existing lighting not providing any illumination during the hours of darkness (i.e., lighting adjacent to the Humanities Building at MVC), bollard lighting was not turned on. Other observations included damaged or

³ <https://www.standardpro.com/how-to-measure-light/>



removed lighting that had not been replaced (i.e., luminaire head missing at NC adjacent to the entry into the Sports Complex parking lot).

General observations per campus are listed as follows:

Moreno Valley College

- Maintenance is required at lighting fixtures where the luminaire fixture is not emitting any light, see Image 1. Power is available as indicated by the other luminaire fixture mounted at the same post.
- Lighting is not consistently placed throughout parking lots, there is some reliance on building mounted light fixtures to illuminate the parking lot areas, see Image 2, at the Dental Center.
- Some areas have excellent lighting as observed at the seating area between the Dental Center classroom blocks, see Image 3.
 - Shadows, and dark spots are eliminated by an even lighting spread, this provides a sense of safety and ease of identifying other pedestrians at night (there were people observed loitering at night).
- Lighting at night reduces 100% the reflective performance feature of glazing film that reduces visibility from the public side during hours of daylight. See Images 4 and 5.
 - Obscured visibility is eliminated when internal lighting is in use during hours of darkness. This will happen any time the light on the inside is brighter than the light on the outside.
 - Lighting is not installed adjacent to all emergency call stations providing ease of reading of any directional instructions displayed.
- Lighting at most main building entry points is particularly good with main building access points easily identifiable at night through lighting. Walkways within the common areas have some reduced lighting with ambient lighting from buildings providing a reduced level illumination. See Image 6.
- Lighting at the walkway adjacent to the Humanities building was poor as the existing bollard lighting was not turned on. Lighting is installed and available, but power was not activated.
- The Learning Gateway access road that provides access to the campus access road is poorly lit as is the access road adjacent to the Library and SAS buildings.
 - Areas of concealment are prevalent with no ability to observe activity visually during hours of darkness as the area is poorly illuminated.
- Lighting illuminating the pedestrian approach to parking Lot E was poor, lighting within the parking lot itself is excellent. See Image 7.
- Street lighting alongside Parkside Lane playing area is sporadic, with shadows specifically on the playing field area.
- Conduct a maintenance review of trees that are overgrown obscuring lighting fixtures, this will provide an immediate positive impact on lighting levels.
- The parking lot directly above the Dental Center is currently undergoing construction and lighting is not available.
 - The lack of lighting due to construction impacts ambient lighting levels that would be provided.



Image 1, Image 2, Image 3



Images 4, Image 5, Image 6



Image 7

Norco College

- Lighting across the Sports Complex field area is not installed providing no visibility of activity once nightfall sets in.
- General parking lot lighting across Parking Lots A and B is strong with well spread lighting distribution that benefits from the new asphalt and line markings reflecting lighting. See Image 8.
- Parking Lots C and D lighting is not as effective as Lots A and B, excellent sidewalk located lamp posts illuminate outwards into the parking bays adjacent to West End Drive. See Image 10.
 - Parking lot lighting helps illuminate pole mount emergency call stations that have unlit strobes that do not enhance visibility of call station location. See Image 9.

- The JFK Middle College High School parking lot has several double-headed light fixtures with only one luminaire powered up. The discrepancy in lighting with adjacent college parking lots is noticeable.
 - Maintenance review of one of the luminaires not illuminating when the other side of the head does should be performed, and illumination reinstated.
- General walkway lighting through the inner courtyard area of campus from the Student Services Building to the Applied Technology Building is good. Lighting is distributed by lamp posts evenly although some shadows were noticeable. See Image 13.
- Exterior lighting along Rodeo Road that is wall mounted in the Operations Center provided poor illumination of the sidewalk and road. Several luminaires require repair as they were not all lit.
- Street lighting along Third Street fails to provide an even distribution of light across the roadway, lighting is located on the horse trail side of the road providing illumination back onto the road rather than evenly spread positioning of lamp posts on both sides of the road. See Image 11.
- Illumination of the exterior covered walkways at the courtyard areas adjacent to the Industrial Technology building is excellent and the emergency call station is easily identifiable with a blue strobe permanently illuminated. See Image 12.
- Lighting at night reduces 100% the reflective film performance feature of film that reduces visibility from the public side of the buildings during hours of daylight.
 - Obscured visibility is eliminated when internal lighting is in use during hours of darkness.



Image 8, Image 9, Image 10



Image 11, Image 12, Image 13

Riverside City College

- Application of lighting varies across the campus with some areas of excellent levels of illumination recorded and others with poor levels. It is evident that lighting has been installed on a construction project-by-project basis with different lighting head styles observed. See Image 15.
- Lighting along Saunders Street adjacent to the parking lot is good with several lamp posts emitting exceptional lighting levels that provide illumination bleed and reflection off of the concrete sidewalks and roadway. See Image 17.
- Parking lots and access roadway at the swimming complex provide good levels of illumination. The distance between lamp posts causes some shadows due to the spread of lighting achieved by the luminaires.
- Generally pedestrian walkway lighting is sufficient, and, in some areas, exceptional. Readings were achieved (i.e., the walkways between the Arts and Ceramics buildings from the ground level at the Gymnasium). See Image 19.
- Lighting within the parking garage itself is good with evenly distributed light placement reducing shadows and providing visibility of all activity that is occurring within the structure. See Images 21 and 22.
 - The half-wall construction of the garage allows for visibility without restriction from a distance at night.
 - Lighting on the exterior sidewalk of the parking garage is inconsistent and does not provide any illumination of the adjacent baseball fields or pathways leading to the Ceramics building.
- The Lovekin Complex is, in general, poorly lit with areas of large shadows providing restriction of visibility of potential bad actors. See Image 18.
- Entry points to campus buildings are typically well lit. However, sidewalk illumination is poor, specifically at areas adjacent to the Quad building. Excellent light readings were achieved at select spots but inconsistency in light deployment causes areas of darkness. See Image 20.
- Lighting at the Early Childhood Education Center at the time of assessment provided good readings on the sidewalk leading up Stadium Way to 15th Street. The parking lot lighting levels recorded in the poor range.

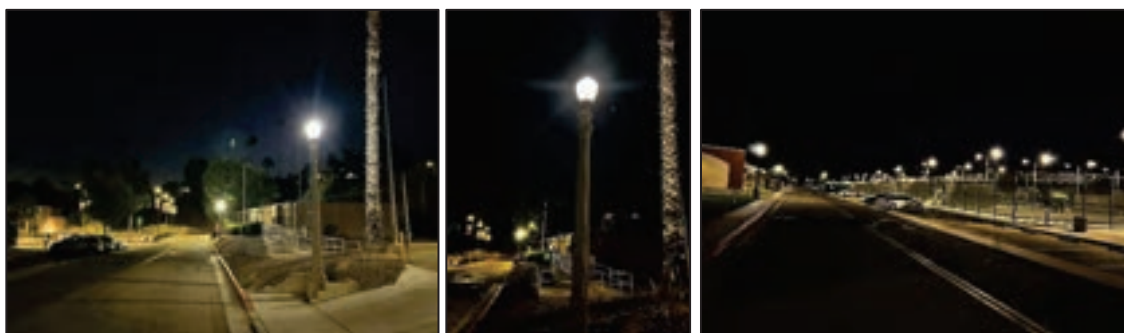


Image 14, Image 15, Image 16



Image 17, Image 18, Image 19



Image 20, Image 21, Image 22

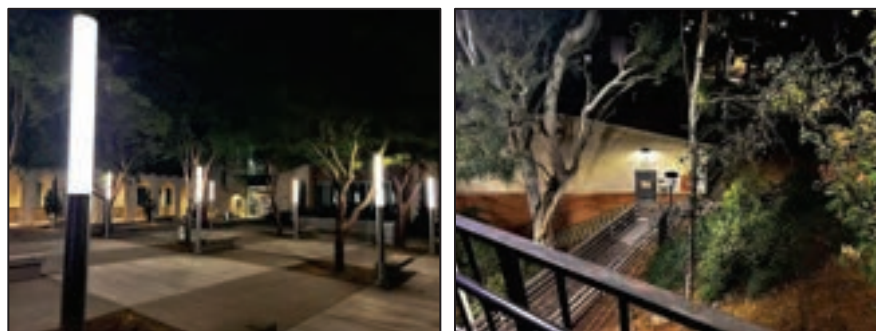


Image 23, Image 24

The assessment team did not feel unsafe due to the lighting levels observed at any point at each of the campuses. However, there are areas that need improvement. Safety perceptions might have been different if the assessment had been conducted during late evening or early morning hours or by a single individual instead of a pair of assessors. Good lighting at MVC allowed for the identification of individuals who seemed out of place at night, particularly near the open restrooms outside the Dental Center. The construction activity across the sites naturally affected the recorded lighting levels, with several areas lacking lighting due to this. This temporary decrease in lighting impacts on the typical illumination, as areas with reduced lighting due to construction may inadvertently affect the lighting of nearby areas.



Considerations

In addressing lighting inconsistencies across a college campus, it is crucial to recognize the far-reaching implications on safety, aesthetics, energy efficiency, and navigation. Ensuring well-lit areas, implementing energy-efficient lighting technologies, and developing a cohesive lighting plan will not only mitigate these concerns but also foster a more secure, inviting, and efficient campus environment for all.

Security electronics technology such as video surveillance should be supported by consistent lighting. Exterior lighting should be uniform rather than bright cones of light interspersed in areas of darkness. Where exterior lighting is low or inadequate and existing video surveillance cameras do not have infra-red (IR) capability, it is recommended that remediation activity first attempts to resolve video surveillance lack of visibility at night with either the addition of further exterior lighting, and or consideration of replacement of existing cameras with installation of camera models with extreme low-light day/night capabilities, wide dynamic range, or with built-in infrared illumination. Adding lighting to areas where cameras are installed can have secondary benefits such as increasing the perception by persons with ill intent that they may be observed.

Landscaping in general across all campuses supports natural surveillance with CPTED best practice of ground coverings remaining below 2' in height and tree canopies above 6' commonplace. There are areas as documented within the individual reports that attention to overgrowth is required regarding ground covering above 2' and trees that mask lighting illumination that require cutting back. Review of light fixtures that are damaged, lack power, or require replacement/reinstallation is encouraged. The use of Light-Emitting-Diode (LED) light fixtures provides energy efficiency and the great majority of lighting across all campuses has transitioned to LEDs, but fixture types vary as with other security applications on a project-by-project basis. It is recommended that there should be a standardized approach to lighting fixtures (i.e., wall mount sconces, lamp post, bollard lights etc.) from a product perspective be implemented. Applying fixtures that have a consistent appearance, performance output, and use in typical applications will support the consistency of community and campus end-user experience across all district sites; outwardly demonstrating ownership of security and safety application by the District.

All three campuses have significant areas of both vehicular and pedestrian use and traditionally lighting evaluations have precedence over vehicle visual needs than those of pedestrians. In a campus setting where parking lots are on the perimeter of the college buildings and pedestrians need to traverse through parking lots requires consideration of pedestrian safety and security needs. The Pacific Northwest National Laboratory (PNNL) published a 2013 report identifying five primary variables that influence pedestrian's impressions of outdoor lighting, these are:

- **Luminaire** – attractive and context-appropriate daytime luminaire appearance
- **Glare** – glare was the most “significant” determining factor in luminaire favorability.
- **Distribution** – pedestrians preferred more uniform light distribution with soft edges.
- **Color temperature** – pedestrians preferred light with warmer color temperatures (2700k-3000k)
- **Horizontal illuminance** – illuminance measures at the low end of the Illuminating Engineering Society (IES) spectrum were acceptable as long as glare was minimized.



Known pedestrian perspective of outdoor lighting application along with the information displayed in Table 7, illustrating average lighting levels as recommended by the IES for exterior parking garages, lots and building exterior, should serve as a minimum baseline condition that lighting provides across all campus and facility exteriors.

Application and Task	Maintained Horizontal		Maintained Vertical		Comments
	Average (fc)1	Range (fc)2	Average (fc)1	Range (fc)2	
EDUCATIONAL EXTERIOR					
Parking (Covered)	5	-	-	-	1 Min; 10:1 Max-Min Uniformity
Parking (Uncovered) Zone 3 (Urban)	1.5	0.75 - 3	0.8	0.4 - 1.6	
Parking (Uncovered) Zone 2 (Suburban)	1	0.5 - 2	0.6	0.3 - 1.2	
Safety (Building Exterior)	1	0.5 - 2	-	-	For security issues, raise Avg to 3

Table 74 - IES Exterior Lighting Foot-Candle Recommendations

Key factors that the district may consider when refreshing or adding additional exterior lighting are:

- Review legacy non-LED lighting fixtures, will they support transition into LEDs, or do they require replacement of the fixture as legacy lighting that was intended to provide omnidirectional lighting rather than directional.
- Review wall pack lighting distribution, do they provide bright spots immediately above openings with little illumination of the wider area?
- Application of bollard lighting, review the height of the lighting as bollards are easily reachable and can be subject to vandalism. Identify the intent of bollard lighting, is it to support pedestrian navigation and is it complimentary to other lighting installed i.e., pole mount fixtures.
- Review application of accent lighting, is accent lighting the only means of providing illumination to an area or is it supported by other lighting fixtures.
- Use cut-off lighting fixtures minimizing light pollution. Use white light sources and avoid glare.
- Apply lighting consistently to support CPTED fight or flight concept. Visibility of at least 30' should be available to allow pedestrians to make immediate decisions if they encounter a potential situation of concern.

It is recommended that a lighting consultant be engaged to provide subject matter expertise and guidance regarding appropriate lighting placement, and illumination levels as it pertains to regulatory requirements.



Policy and Procedure Review

Policies and procedures serve as a guiding framework for decision-making and facilitate the standardization and optimization of internal processes across all operational sites.

The SOBE/Aanko review of policy and procedures is restricted to documentation related to safety and security as provided directly by the district. At the time of review the district is also concurrent with this project performing an internal review and refresh of policy and procedure documentation. Each policy and procedure review was performed compared with relevant code and regulations.

Policy No. 5700 Use of Facilities and Grounds

This District Policy references California Education Code Sections 82537 and 82542 and the California Code of Regulations Section 59601. The current district policy aligns with these codes, however there is one section that needs clarification.

In the 4th paragraph there are quotation marks around language that references the California Education Code 82537 (a). This information is not consistent with the current language in that section of the Education Code. The district should consider revising the policy to align with current Education Code language.

Procedure No. 5700 Use of Facilities and Grounds

This District Procedure references California Education Code Sections 82537 and 82542 and the California Public Resources Code Section 42648.3. The current district procedure aligns with these codes, however there is one area that is not noted in the procedure. There is no mention of how the funds are collected and deposited into a special fund.

California Code of Regulations Section 59606 requires “Funds collected by a community college district as capital direct costs shall be deposited into a special fund that shall only be used for capital maintenance, repair, restoration, refurbishment, or replacement.” The district should consider adding this language to the next revision of this procedure.

The current procedure has language regarding the use of district facilities for mass care and welfare shelters during disasters. The district campuses are not set up to provide this service and it is recommended to remove this language.

Policy No. 5520 Security for District Property

The District Policy references California Education Code Sections 81600 et seq. and the current district policy aligns with this code.



Procedure No. 5520 Security for District Policy

The district did not supply a copy of the procedure associated with this policy. If a procedure is not in place, then the district should complete a procedure utilizing California Education Code Sections 81600 et seq. as a guideline.

Policy No. 5800 Campus Safety

This District Policy references California Education Code Sections 67380(a)(4) as the guiding document for this policy. The information contained in the policy is in line with this section of the code. The section cited is only a small part of the overall requirements of the Education Code related to campus safety and the district has developed additional separate policies and procedures to address most of these requirements.

Procedure No. 5800 Campus Safety

The District Procedure references sections of the Education Code, the Penal Code, Code of Federal Regulations, and the Campus Security Act of 1990 as guiding documents for this procedure. The information contained in the procedure is in line with the guiding documents.

The Safety Plan Brochure and the Annual Report completed by the Police Chief to the Board of Trustees were also reviewed and found to be compliant with reporting requirements.

Policy No. 5810 Workplace Violence and Safety

The District Policy references the Workplace Violence Safety Act of 1994" (Code of Civil Procedure Section 527.8 and Penal Code Section 273.6); Cal/OSHA: Labor Code Sections 6300 et seq.; 8 California Code of Regulations Section 3203. The current district policy is being reviewed for compliance with these code requirements.

Procedure No. 5810 Workplace Violence and Safety

The District Procedure references Cal/OSHA- LaborCodeSections6300et seq.; Title 8 Section3203; Code of Civil Procedure Section 527.8; Penal Code Sections 273.6, 626.9, 626.10, and 12021 as guiding documents. The current district procedure is being reviewed for compliance with these code requirements.

Electronic copies of restraining orders/court orders are managed by the Riverside County Sheriff's Office and are available to the District Police when needed.

Training on this policy and procedure is being worked on by HR and the PD and a program for the training is scheduled to be released.



The policy and procedure should include the Deputy Title IX Coordinator. This person is noted in the District's Clery Act Report as receiving a copy of court orders. The Police Chief will review this information so that there is consistency.

Policy No. 5818 Child Abuse Reporting

The District Policy references Penal Code Sections 261, 264.1, 273a, 273d, 285, 286, 288, 288a, 289, 601, 647a, and 11164-11174.3; Welfare and Institutions Code Sections 300 and 318; Family Code Sections 7802, 7807, 7808, 7820-7829, 7890, and 7892 as guiding documents. The current district policy aligns with these code requirements.

Procedure No. 5818 Child Abuse Reporting

The District Procedure references Penal Code Sections 261, 264.1, 273a, 273d, 285, 286, 288, 288a, 289, 601, 647a, and 11164-11174.3; Welfare and Institutions Code Sections 300 and 318; Family Code Sections 7802, 7807, 7808, 7820-7829, 7890, and 7892 as guiding documents. The current district procedures align with these code requirements.

The District maintains copies of signed statements by employees who are designated as a mandated reporter. HR should manage this program and the associated files.

Policy No. 5815 Reporting of Crimes

The District Policy references Education Code Section 67380; 34 Code of Federal Regulations Section 668.46(b)(7) as guiding documents. The current district policy aligns with these code requirements.

The district should add the following information as a reference document and in the body of the policy: Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1998.

Procedure No. 5815 Reporting of Crimes

The District Procedures reference Penal Code Sections 245 and 422.55; Education Code Sections 212, 67380, 67383 and 87014; Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1998; 20 U.S.C. § 1232g; 34 C.F.R. 668.46; 34 C.F.R. 99.31(a)(13), (14) and 668.46; Campus Security Act of 1990 as guiding documents. The current district procedures align with these requirements.

The district should utilize all the information contained in California Education Code, Title 3, Division 5, Part 40, Chapter 15.5 Student Safety as the guiding document for this policy and procedure. Special attention should be given to Sections 67380-67386.



Policy No. 5830 Weapons On Campus

The District Policy references Penal Code Sections 626.9 and 626.10 as guiding documents. The current district policy aligns with these code requirements with one exception. There are exceptions to the Penal Code in Section 626.9 as well as 626.10 and that information should be added to the district policy.

Procedure No. 5830 Weapons on Campus

The District Procedure references Penal Code Sections 626.9(h) and (i), 626.10(b), 16780 and 17230 as guiding documents. The current district procedure aligns with these requirements with the following exception. The list of weapons in paragraph three does not include all weapons listed in the penal code. The procedure should also include razors, stun guns, a folding knife with a blade that locks into place, or a switch blade or butterfly knife.

Policy No. 5801 Campus Security and Access

The District Policy references 34 Code of Federal Regulations Section 668.46(b)(3) ACCJC Accreditation Standard III.B.1 as guiding documents.

These guidelines are closely related to campus safety. The district should consider removing this policy and incorporating the referenced guiding documents into District Policy No. 5800 Campus Safety.

Procedure No. 5801 Campus Security and Access

The District Procedure for this policy was not provided. The district should consider removing this procedure and incorporating the referenced guiding documents into District Procedure No. 5800 Campus Safety.

Policy No. 5950 District Police

The District Policy references Education Code Sections 72330 et seq. and Government Code Sections 3300 et seq as guiding documents. The current district policy aligns with these requirements, but the district may not be aware of what the guiding documents mean for district law enforcement officers.

The district should be aware that Government Code Section 3300, also known as the Peace Officer Bill of Rights, outlines certain rights and protections for peace officers. It is recommended that Human Resources review this section of the Government Code and if needed, revise both the policy and procedure to align with the code.



Procedure No. 5950 District Police

The District Procedure references Education Code Sections 72330 and 72330.2 and Government Code Sections 3300 et seq as guiding documents. The current district procedure aligns with these requirements. Information regarding the Peace Officers Bill of Rights is noted above.

Related to this procedure, it appears the district hired Lexipol to write the Riverside Community College District Safety and Police Department Procedure Manual in 2021. A review of this large document should be completed to ensure consistency with district polices related to law enforcement.

Policy No. 5820 Local Law Enforcement

The District Policy references Education Code Section 67381 and 34 Code of Federal Regulations Part 668.46(b)(4) as guiding documents. The current district policy aligns with these requirements.

Procedure No. 5820 Local Law Enforcement

The District Procedure references Education Code Section 67381 as a guiding document. The current district procedure aligns with these requirements.

Policy No. 5840 Sexual and Other Assaults on Campus

The current District Policy references 20 U.S.C. Section 1092(f); Education Code Sections 67382, 67385, and 67386; and 34 Code of Federal Regulations Section 668.46(b)(11) as guiding documents. The current district policy aligns with these requirements.

Procedure No. 5840 Sexual and Other Assaults on Campus

A copy of the procedure was not provided.

Video Surveillance Policy and Procedures

To ensure the successful implementation and continued operation of the video surveillance component within the overall security program, it is essential to establish clear and effective written policies to guide its execution and evaluation. Questions to consider when creating the policy and procedures include:

- What are we doing and why?
- Who can review recordings?
- How long should we store recordings?
- Who can archive or export recordings?



- How long to save events?
- How do we evaluate the effectiveness of the program?
- What is the period of evaluation?
- What are the consequences for violating policies?
- Verbiage and locations for signage indicating use of video surveillance.

The implementation of security video surveillance technology should be complemented by the display of pertinent signage indicating its operation within the area. It is important to note that the presence of this technology does not entail assurances of safety or active monitoring and response. The language used on the signage should be in alignment with the guidance of legal counsel. Examples of suitable wording include "Video Surveillance In-Use" or the depiction of a camera icon without accompanying text.



The Future

ROADMAP

A security program roadmap is a strategic plan for implementing and executing security projects with the aim of achieving an optimal security program state. It details important stages, milestones, and recommendations for enhancing the effectiveness of a security program over time. The following roadmap outlines crucial action items that will provide clear direction, focus, and implementation for the RCCD safety and security program. This roadmap is designed to support the path to enhancement, encompassing governance, operational needs, built environment, and technology perspective. The timeline of approach is dependent on the district's needs to escalate and prioritize activity. The activities are illustrated in order of recommendation for completion, see Figure 7.

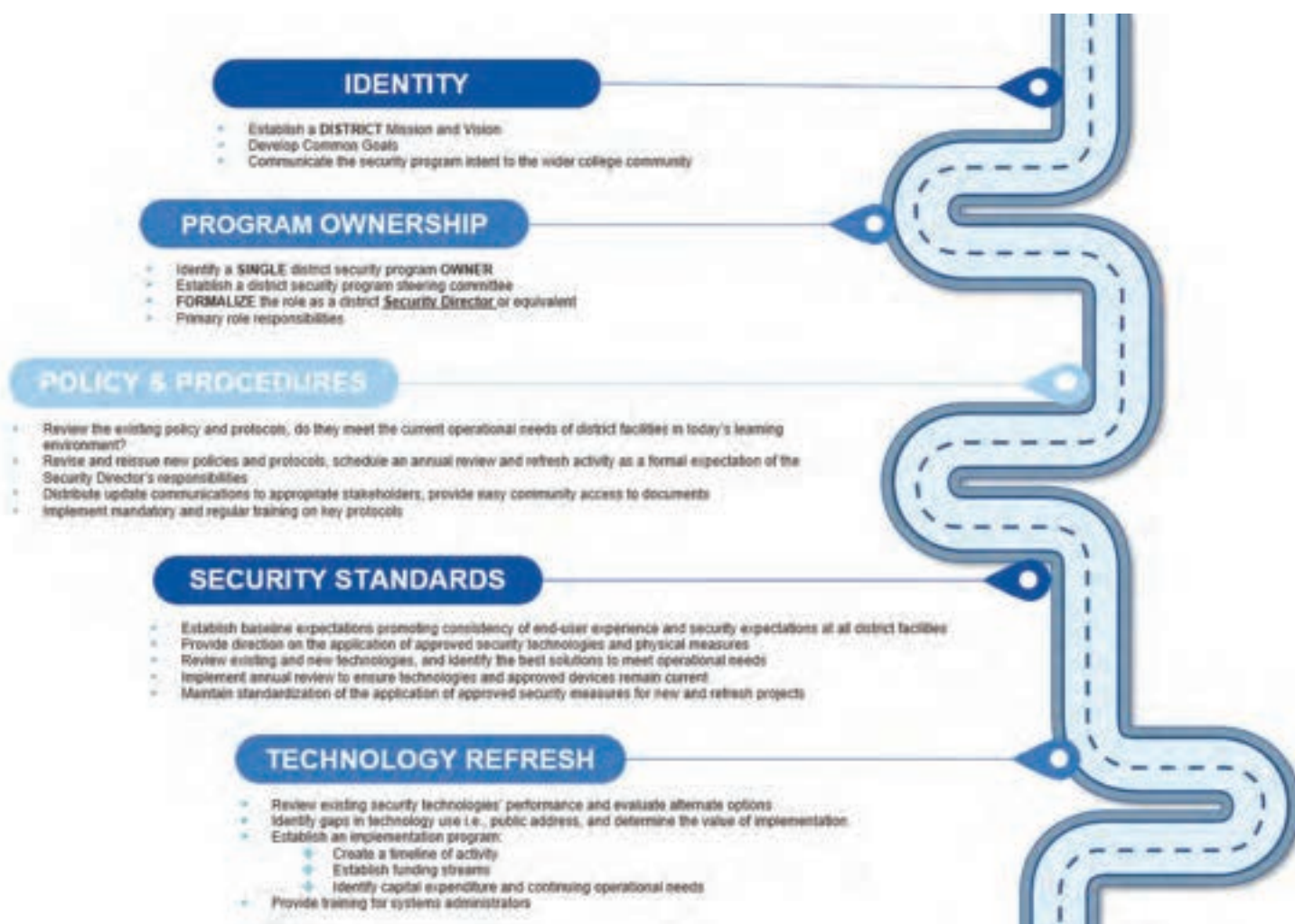


Figure 7 - Roadmap of Activity



IDENTITY, LEADERSHIP AND OWNERSHIP

Identity and leadership are critical to maintaining a safe and conducive learning environment. These components, when in place, may support enhanced reputation and attractiveness of RCCD as a destination learning institute. A centralized management and control approach to security program oversight would offer collective ownership responsible for maintaining policy and procedures, reviewing physical and operational needs, and staffing measures including consulting with district police to review, revise and deliver a memorandum of understanding. A security program charter would formalize practices related to the District's leadership's commitment to establish, implement, maintain, and continuously improve the District security program, especially with respect to program policy, scope, and objectives. The security program governance team should serve as custodians responsible for leading and overseeing the program charter implementation.

SYSTEMS UNIFICATION OR INTEGRATION

It is recommended as detailed prior that the district evaluate both alternate security electronics systems and capability of the incumbent system to at minimum provide integration between access control, intrusion detection, and video surveillance. The existing Software House CCure 9000 access control and the American Dynamics Victor video surveillance systems can be **unified** by transitioning from client workstation login to the CCure IQ cloud platform that unifies the two components. CCure IQ offers flexibility to the district to deploy a set-up that best serves their operational needs. CCure IQ can be set-up with cloud access, be run on-premises, offered as a combination of the two, and can leverage Infrastructure as a Service (IaaS) or Software as a Service (SaaS) models.

Other systems also provide unification capability, and it is recommended that the district evaluate other options as part of any future scaling of security electronics deployment. A thorough evaluation and due diligence process based on preferred infrastructure, operational, and end-user needs is encouraged.

The terms unification and integration are often used interchangeably, but they do not mean the same thing. A unified physical security platform consists of a suite of products developed as one unit. It means you can turn different systems on or off, but you cannot break connections – because there are not any. A unified solution is built from the ground up to consolidate all of the data that you gather, so you can easily and efficiently manage security policies, monitor events, and run investigations.⁴

The evolving use of Artificial Intelligence (AI) and advanced feature sets provides opportunity for abnormal behaviors and activity to be identified by systems software and notifications pushed to the appropriate persons. Using a unified platform further reduces the management of separate integrated components down to a single pane-of-glass, providing systems administration efficiency. Factors to consider within a review process of a unified platform approach include the following pros and cons:

⁴ [Unified vs. integrated physical security solutions \(genetec.com\)](https://www.genetec.com/whitepapers/unified-vs-integrated-physical-security-solutions)



PROS	CONS
Simplified training and maintenance	Potential single point of failure
Reduced complexity and costs	Restricted device options if proprietary solution or feature sets restricted to system manufacturers products
Enhanced use of AI and features sets	Continual development and evolution of system capability locked-in to the manufacturer roadmap for continual progression
Seamless visibility and alarm event notification and response	Pricing may be affected by minimal edge device options
Efficiency in updating of governance documentation	
Ease of scalability to support additional card readers and video surveillance cameras etc.	
Simplification of systems update process	

Table 5 - Pros and Cons of Electronic Unified Security Solutions

Considering the bigger picture perspective, it is important to combine various aspects of the security program beyond just security electronics. This includes bringing together components such as risk management, security staffing, and systems design, as a unified approach to security management. Doing so can offer several benefits to the security program. Amalgamation under a District security program owner, using software where applicable, may provide operational efficiencies, availability, and visibility of information, and support controlled accessibility to authorized personnel for viewing and distributing information. Centralizing and combining security information sharing can improve security intelligence and streamline communication processes, benefiting the districtwide security posture. Additionally, amalgamated management of the holistic security program will support the District's needs to stay compliant with regulatory standards by ensuring that all security measures are aligned across the District facilities and providing a central repository of governance documentation.



Figure 86 - Integrated Security Solutions

SYSTEMS GOVERNANCE

An effective tool for implementing security systems is creating a device placement standards matrix. The matrix can serve as a baseline reference for the initial device placement and consideration of security electronics components on all retrofit and new construction projects. A matrix, when used in conjunction with written narrative standards, can provide a comprehensive Division 28 approach for the district. Developing security standards ensures consideration of Division 28 application on all new and retrofit projects when mandated by board policy. It is recommended that any desired or requested deviation from the approved standards requires the approval of the RCCD proposed security program owner (or Chief of District Police). All Division 28 applications should require the District’s security program owner review and approval prior to acceptance of any formal security electronics design being issued for contractor bid or in-house installation.

Tools such as a matrix should be reviewed and revised annually by the proposed DSC as the safety and security program evolves and operational needs may change. Division 28 standards and performance specifications, if created, will also require continual review and revision ensuring that current supported systems software and edge devices are documented.

Governance of security electronics systems is a fundamental element of the security program that provides control and direction ensuring:

- Consistency of systems deployment
- Management of safety and security measures that may affect operational functionality of the built environment.
- Reference for retrofit and new construction design and operational needs



- Control of the environment culturally in respect to safety and security management using technology
- Support of the wider communication of safety and security expectations across the District to end-users and promotion of a sense of end user familiarity with safety and security measures
- Appropriate protocol on systems and consequence for misuse

SYSTEMS MAINTENANCE AND PERFORMANCE CHECKS

An important element of governance is the controlled scheduling of performance verification and maintenance of both communications and security electronics systems. Performance of critical communications and security systems should not falter. A regular verification of performance is recommended as a scheduled activity to ensure that performance is as expected, and any identified issues can be remediated with urgency and efficiency. A lack of regular systems testing presents potential risk to the district. If an emergency requires the utilization of communications and security electronics systems and they fail due to lack of frequent and documented maintenance and performance testing. This could be a significant problem for the district should there be a harmful occurrence. There were examples of systems performing poorly during the assessment, specifically emergency call stations and video surveillance cameras. It is recommended that systems and components identified as non-operational intended to serve safety and security emergency incident response and visibility be remediated immediately. Frequent testing is a cost-effective measure comparative to potential bigger picture liability considerations.

An additional recommendation is the upkeep of software support agreements (SSAs) that serve as a legal contract that obligates systems vendors to provide technical support and updates for their software products for customers. Centralized management of SSAs is recommended to make certain that all agreements provide the same levels of service and support across all RCCD campuses and administrative facilities. The existing localized procurement and management of SSAs results in differing software versions and contractor support experienced. A centralized management approach further ensures that each campus can request the same level of technical support and assistance from systems manufacturers, local budgeting should not determine the support provided to communications and security electronics systems regardless of location.

Within the education sector many security technology vendors will provide SSAs for a predetermined period, i.e., 5 years, allowing districts to capture costs within capital expenditures project budgets. Lapse of SSAs can have significant detrimental systems performance and cost impact in the future. Often systems software advanced features are not made available when SSAs lapse, which in turn could negate the district's ability to maximize systems advanced features to benefit the security program.

DIVISION 28 STANDARDS

It is recommended that RCCD engage a security professional for support and development of formal Division 28 Safety and Security standards that take a district level baseline conditions approach, rolled out across separate college campuses and administrative buildings. The implementation of a standardized baseline approach of security electronics in predetermined locations/applications does not eliminate unique and nuanced needs of individual campus and facilities. They simply provide a commonality of approach that ensures that overarching district



expectations, security goals and mission are delivered without deviation unless approved by the security program owner.

Newly developed standards should serve as the governance reference for a phased upgrade of all RCCD campus and administrative buildings (as needed) to deliver a minimum baseline implementation and user experience of all buildings in compliance with Division 28 standards. Analysis of existing conditions and upgrades needed to meet approved standards may be required, to support development and establishment of future spend requirements to support such an implementation project.

It is recommended that the district does not overlook governance and mitigates the pitfalls of implementation of an integrated security electronics system/program without controls. Standards will set expectations of use and promote a commonality of campus user experience related to electronic security measures. Security electronics technology should serve the RCCD with an operational benefit and force-multiplication to existing physical security staffing and policing measures.

In addition to Division 28 Safety and Security standards, the district may also consider creating a complete physical security program set of standards to provide guidance on minimum baseline expectations for all other measures. *These physical security standards are critical as they promote consistency of security measures and provide*⁵.

- **Deterrence:** Standards function as a deterrent against criminal activities by establishing clear security protocols and expectations.
- **Protection:** They safeguard personnel, property, data, and physical assets against threats like theft, vandalism, and terrorism.
- **Compliance:** Standards help organizations comply with regulations and industry-specific security mandates.
- **Risk Mitigation:** By identifying vulnerabilities and determining how to mitigate risks, standards enhance overall security.
- **Benchmarking:** They promote best practices and allow organizations to benchmark their performance.

⁵ [Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide - December 2015 \(cisa.gov\)](#)



APPENDIX A – STAKEHOLDER PERSPECTIVE (IN-DEPTH NOTES)



Key Themes and Observations

1. Campus Security Presence and Engagement of Police Department

A unique aspect of the Riverside Community College District is the presence of its own full-time law enforcement agency, which is an advantage over other similar institutions. Most campus physical security assessments do not involve conversations regarding law enforcement other than coordination with local agencies if events occur. Due to this difference, the likelihood of the campus police coming up in conversation concerning security was extremely high. There were many comments regarding the police department and its perceived effectiveness within the district organization. The assessment team did its best to stay on topic about security, and we recommend that the campus police may warrant further examination.

Across the interviews, participants consistently reported concerns regarding the visibility and effectiveness of campus police. Many interviewees highlighted the stark reduction in law enforcement presence, particularly after dark, in secluded areas such as parking lots, STEM centers, and lesser-used classrooms. The lack of visible security officers has contributed to a heightened sense of vulnerability among students, staff, and faculty.

Several stakeholders recalled a time when campus police were more integrated into the community, fostering a relationship of trust with students and staff. This proactive engagement was perceived as a deterrent to crime and a reassurance to campus residents. However, interviewees expressed concern that this engagement has diminished over the past few years, with officers now primarily remaining in patrol vehicles or responding reactively to incidents rather than proactively patrolling campus grounds.

One faculty member shared an incident where a law enforcement pursuit ended on campus, sparking concern about the campus's preparedness for such unpredictable, high-stakes situations. Another interviewee noted that the decrease in public safety personnel on campus coincided with budget cuts, leaving security stretched thin. Although some campuses experienced a slight increase in police visibility this semester, it was broadly agreed that this presence was inconsistent and largely concentrated during the busiest daytime hours.

A significant part of the discussions also revolved around internal challenges within the police department, including high turnover rates, leadership instability, and staff shortages. Multiple interviewees raised concerns about the inconsistent and sometimes slow response times from campus police, leading to a breakdown in trust between the department and the campus community. One staff member recounted an incident involving a vandalism event where response times were delayed, further fueling frustration about police availability.

2. Communication and Incident Reporting Deficiencies

Communication breakdowns were highlighted as a major area of concern across the campuses. Many participants described situations where important information regarding security incidents—such as thefts, vandalism, or disruptions—was communicated poorly, if at all. This lack of timely, structured communication created anxiety among campus residents, who often had to rely on informal channels to stay informed about incidents. A number of interviewees referenced incidents where rumors spread quickly due to the absence of clear and consistent information from the administration or campus police.



For instance, there was a consensus among several interviewees that campus communication systems need to be reformed to provide faster, clearer notifications during emergencies. Participants mentioned the absence of follow-up messages after incidents, which left many uncertain about the status of the situation. One interviewee recalled a fire alarm incident where confusion and lack of communication led to unnecessary panic among students and staff.

Additionally, the reporting process for non-emergency incidents, such as suspicious activity or minor property damage, was deemed cumbersome. Faculty members reported long wait times when attempting to report incidents through the existing system, which discouraged them from filing reports unless absolutely necessary. Several participants suggested the need for a mobile app or a more user-friendly platform to facilitate incident reporting and communication with campus safety personnel.

3. Physical Security Infrastructure and Vulnerabilities

Concerns about the physical security of campuses were raised repeatedly. Interviewees highlighted multiple areas where security infrastructure, such as lighting, surveillance cameras, and access control systems, was either inadequate or malfunctioning. The open layout of some campuses was described as a particular vulnerability, with poor lighting in parking lots, pedestrian walkways, and remote classroom areas posing significant safety risks, particularly at night.

One of the most common points of feedback concerned the surveillance systems on campus. Many participants noted that some cameras were either not operational or not adequately monitored, leading to security gaps in key areas. One staff member recounted an incident in which vandalism near portable classrooms was captured by a non-functional camera, rendering the footage useless for investigation. There were also reports of security cameras that were not well-positioned, with some only covering limited portions of high-traffic areas while ignoring more vulnerable spots.

Access control was another key area of concern. Interviewees described issues with outdated key-based systems, advocating for the installation of electronic key card systems to regulate access to sensitive areas. Several participants pointed out that certain campus buildings, particularly older ones, did not have secure ingress and egress points, making them vulnerable to unauthorized entry. For example, one building was described as having a single point of entry, raising concerns about bottlenecks during emergency evacuations or lockdown situations.

Recommendations for physical improvements were common, with participants suggesting that more should be done to secure buildings through improved lighting, fencing, and remote locking capabilities. These suggestions were accompanied by calls for better maintenance of current infrastructure, particularly with regard to ensuring that all security cameras and emergency phones were fully operational at all times.

4. Emergency Preparedness and Inconsistent Training

One of the most consistent themes that emerged from the interviews was the lack of comprehensive and consistent safety training participation in district provided events by faculty and staff across campuses. While some faculty and staff reported having participated in lockdown drills or active shooter training, the overwhelming consensus was that such training effectiveness was minimized as they are not mandatory and often lacked follow-up. Several interviewees inaccurately mentioned that safety drills were only offered to certain groups or departments, leaving large portions of the campus population without crucial emergency response knowledge. The district offers drills to all campuses and



buildings, it is evident that there is a breakdown in the communication of drill activities available to all campus users across the district.

The inadequacy of active shooter drills was particularly noted. Some interviewees criticized the use of live sound effects during drills, citing the trauma it caused to participants, particularly those who had experienced violence in the past. Faculty members also pointed out that while they were aware of the existence of emergency protocols, they were often unclear about their specific roles during an actual incident.

Beyond lockdown and active shooter scenarios, there was widespread concern that campuses were ill-prepared for a range of potential emergencies, including natural disasters, hazardous materials incidents, and medical emergencies. Several interviewees mentioned the need for more frequent training sessions that would allow faculty and staff to practice emergency responses under realistic conditions. The district has offered districtwide more than 50 emergency event trainings since July 2023. As with the availability of emergency drills communication of scheduled session and availability requires review.

There was also significant feedback about the lack of clarity regarding leadership roles during emergency situations. This lack of structure has led to confusion during past incidents, with participants noting that there is often uncertainty about who is in charge of coordinating response efforts.

5. Student Mental Health and Its Impact on Campus Safety

Concerns about the mental health and well-being of students were frequently raised during the interviews. Many faculty and staff noted a marked increase in anxiety and mental health issues among students in recent years, particularly in the aftermath of the COVID-19 pandemic. There were also concerns that students with untreated mental health issues could pose a safety risk to themselves and others on campus.

Participants highlighted several cases where students exhibited signs of distress or disruptive behavior, but the response from campus safety and student services was either delayed or inadequate. Interviewees emphasized the need for greater coordination between mental health services, student affairs, and campus police to ensure that students receive the support they need before situations escalate.

There was also a call for better mental health resources to be made available on campus, particularly for students who may be experiencing trauma or heightened anxiety. Faculty expressed a desire for more mental health training so that they could better recognize warning signs and intervene appropriately when students are in crisis. The need for de-escalation training was also frequently mentioned, with several participants advocating for staff, particularly those in frontline roles, to receive training on how to handle tense or potentially violent situations.

Recommendations for Improvement

Across the interviews, several clear recommendations emerged for improving campus safety and security. The recommendations reflected both immediate needs—such as increasing police visibility and upgrading security infrastructure—and longer-term solutions focused on improving training and mental health support.



1. **Mandatory Safety and Emergency Training:** The most frequently mentioned recommendation was the implementation of regular, mandatory safety and emergency response training for all staff, faculty, and administrators.
2. **Increased Public Safety Presence:** Many interviewees called for an increase in the number of visible public safety officers, particularly during evening hours and in less populated areas of campus. Stakeholders felt that a stronger and more approachable campus safety force would help to deter crime and provide reassurance to students and staff.
3. **Improved Communication Protocols:** Several participants recommended the creation of a more structured communication system for reporting incidents and disseminating information during emergencies. This could include automated follow-up notifications after incidents, as well as a more user-friendly platform for faculty and staff to report security concerns.
4. **Upgraded Security Infrastructure:** Interviewees widely agreed on the need to upgrade physical security systems on campus. This included the installation of key card access systems, the expansion of surveillance camera coverage, and the improvement of lighting in parking lots and walkways. Many participants also suggested that emergency phones and other critical security equipment should be regularly tested to ensure functionality.
5. **Expansion of Mental Health Services:** Several interviewees recommended increasing mental health resources for students, particularly in light of the rising rates of anxiety and trauma. This could include expanding counseling services, offering mental health first-aid training for faculty, and improving coordination between mental health professionals and campus safety officers.

Categorization of Observations and Recommendations by Frequency

Most Frequent Observations:

- **Lack of Visible Campus Police Presence:** (16 mentions) Respondents frequently noted the absence of a visible and engaged police presence on campus, particularly during the evening.
- **Communication Gaps and Delays:** (15 mentions) Issues surrounding the delayed reporting of incidents and poor follow-up communication were common across multiple campuses.
- **Inconsistent and Insufficient Emergency Training:** (14 mentions) Many faculty and staff expressed frustration with the lack of consistent, mandatory training on emergency response procedures.
- **Inadequate Physical Security:** (12 mentions) Concerns about malfunctioning security cameras, poor lighting, and outdated access control systems were frequently raised.

Most Frequent Recommendations:

- **Mandatory Safety and Emergency Training:** (17 recommendations) There was strong support for requiring all campus personnel to undergo regular training on emergency response.
- **Increased Police Visibility:** (16 recommendations) Many participants suggested increasing the number of visible police officers on campus to enhance security and reduce anxiety.



- **Improved Communication Systems:** (14 recommendations) Interviewees recommended implementing structured and timely communication protocols for both routine and emergency situations.
- **Upgraded Security Infrastructure:** (12 recommendations) Participants consistently called for improvements in physical security, including better lighting, key card systems, and operational cameras.
- **Expanded Mental Health Resources:** (8 recommendations) Several interviewees emphasized the need for more comprehensive mental health services and training for faculty and staff to manage crises effectively.



APPENDIX B – PERCEPTIONS SURVEY (STUDENTS AND EMPLOYEES)



A total of four-hundred and eighty-five (485) responses were submitted during an open survey period of two (2) weeks between September 13, 2024, and September 27, 2024. The following analysis includes charts and graphs generated by the survey responses directly within Microsoft Forms.

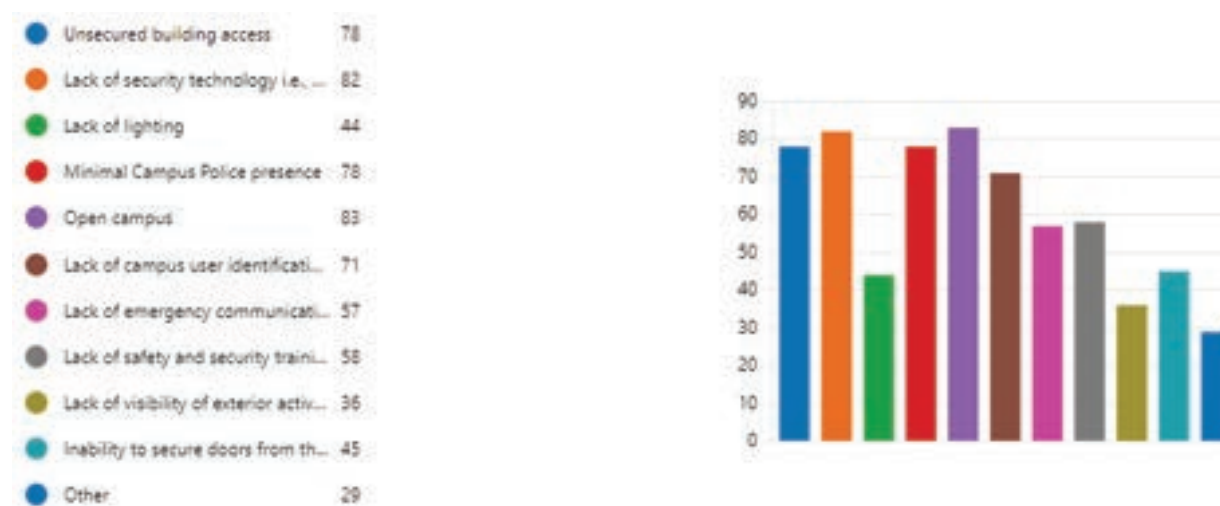
Students

Student response to the survey resulted in two hundred and thirty-six (236) participants with an average time to complete of thirty-two (32) minutes. RCC students were the most responsive with 151 providing their input regarding safety and security.

Q1. Facility/Campus that you are most associated with, select one only.



Q2. From your perspective what concerns you most about safety and security across the college district? Select all that apply.

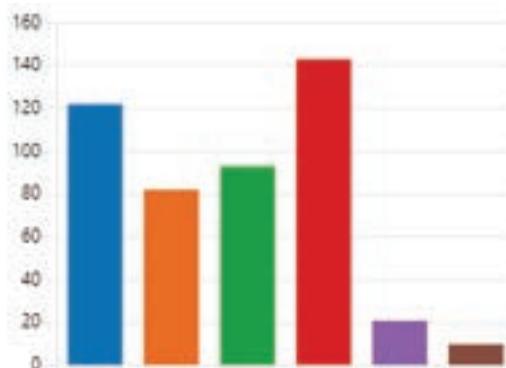


Q4. Have you encountered any security incidents or threats at the campus/facility? If so, can you describe them?

Responses to this open-ended question included several references specifically related to wider social environment issues including homelessness, mental health issues, transients with weapons, and general crime including car break-ins. Several respondents advised that they felt unsafe in poorly lit parking lots without providing additional detail of why such responses are subjective to each individual.



Q5. What is your perception of the strengths of the current safety and security program, what does the district do well? Select all that apply.



Q6. Are there immediate areas of concern that you feel needs to be addressed?

Responses to this open question provided a wide ranging response that included operational, physical, and built environment areas for improvement. There was a consistency in topics raised by students with a theme for more security staffing and campus police presence. Requests for further emergency incident training beyond what is already provided by the district, and improvement in communications related to safety and security.

Q8. Do you know about any incident where emergency help has been required and the ability to communicate effectively to request help has been an issue?

More than 95% of respondents indicated that they had no incident to recall that required them to request help with effective communication being an issue. Specific individual comments referenced slow response from campus security when calls were made, and also identified the non-operational blue strobes at emergency call stations that do not function correctly when calls placed. Individual comments were minimal in the responses but do provide opportunity to address areas deemed requiring improvement by students.

Q9. How often are you actively engaged in training, drills, education, and updates on safety and security?



Q10. Have you ever encountered situations where your own or other's sense of safety and security has been compromised?

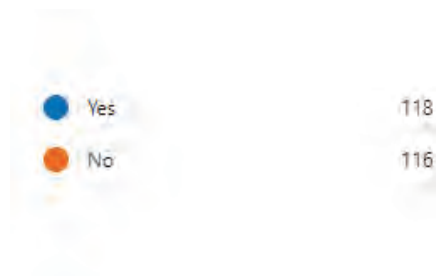
80% of respondents identified that they had not encountered any situation where their own safety and security or that of others had been compromised. Those that did identify that they had encountered situations provided single lien responses that included a wide range of situations including:

- Assault
- Groped in the parking lot
- People asking for cash then stealing items when non made available to them
- Fellow students who behave creepy but not enough to report
- Professor letting students leave class during a lockdown
- Lack of hearing communication over PA
- Unhoused becoming aggressive

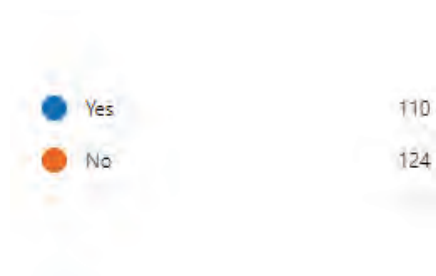
Q12. Are there any areas at the campus/facility where you feel security is lacking?

- Coil Arts Center (15)
- Parking Garage (14)
- Police interaction and behavior is not inviting and lacking (6)
- Open nature is concerning too easily accessible (10)
- Shared gender bathrooms are concerning (1)
- Lack of cameras in parking lots (11)
-
- Non-operating blue lights and phones is concerning (2)

Q13. Are you familiar with the college/facility emergency procedures, such as what to do in the event of a fire, active shooter, or severe weather?



Q17. Do you know how to report a security incident or suspicious activity?



Q21. Are you aware of the locations of emergency call stations on campus or at the facility?



Q23. How do you typically receive security alerts or updates from the college/facility?

- RAVE
- Text
- None
- Phone call
- Emails

Q25. What specific improvements would you suggest enhancing your feeling of safety at the campus/facility? List your top 3.

- Police and CSO presence (38)
- Access control at all buildings (16)
- ID use (10)
- Lighting (18)
- Cameras (45)
- Communication (5)
- Safety Training (14)
-
- More gates to restrict access (2)

Students identified several security improvements they would like to see on campus with the most prominent themes indicated by the quantities above.



Employees

Employee response to the survey resulted in two-hundred and forty-nine (249) participants with an average time to complete of twenty-six (26) minutes. Employees at RCC were the most responsive, with one hundred and twenty-seven (127) providing their input regarding safety and security.

Q2. Stakeholder Role



Employee responses were represented by several groups with Faculty and Classified/Confidential Professionals accounting for over two hundred (200) responses.

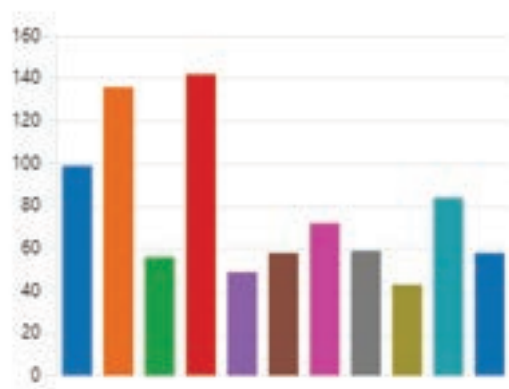
LOCATION AND ROLE	COUNT OF STAKEHOLDER ROLE
Ben Clark Training Center (Buildings #3 and #5)	
Classified or Confidential Professionals	3
Culinary Arts Academy and Riverside Community College District Office	
Administrators	10
Classified or Confidential Professionals	17
Faculty	1
Henry W. and Alice Edna Coil School for the Arts	
Administrators	1
Classified or Confidential Professionals	4
Faculty	8
Moreno Valley College	
Other	3
Administrators	4
Classified or Confidential Professionals	17
Faculty	16
Norco College	
Administrators	6
Classified or Confidential Professionals	18
Faculty	14
Riverside City College	
Administrators	11
Classified or Confidential Professionals	36
Faculty	80
Total Responses	249

Table 9 – Employee Survey Participation by Location and Role



Q3. From your perspective what concerns you most about safety and security across the college district? Select all that apply.

Unsecured building access	99
Lack of security technology i.e., ...	136
Lack of lighting	56
Minimal Campus Police presence	142
Open campus	49
Lack of campus user identificati...	58
Lack of emergency communicati...	72
Lack of safety and security traini...	59
Lack of visibility of exterior activ...	43
Inability to secure doors from th...	84
Other	58



Q5. Have you encountered any security incidents or threats at the campus/facility? If so, can you describe them?

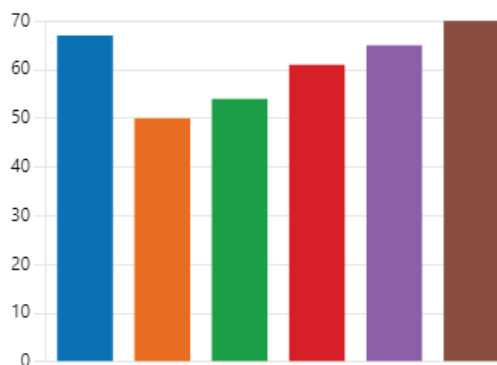
The responses to the open ended question were wide ranging with responses that varied from communication issues to experiencing drug usage by community members. Several responses provided are listed:

- Community member drug use
- Suspicious behavior of homeless/transients
- Fact that RCC Police dispatch is offsite is a problem as dispatch have no familiarity with campus
- Being placed on hold for 20 minutes when contacting campus police for support to deal with a student behaving strangely
- Constant issues at downtown Riverside location at Culinary Restaurant
- Irate students at Student Services Department, lack of Police recognition of situations
- No ability to lock/unlock doors, waiting an hour for response
- Everyone has keys, room accessed when locked in a lockdown!
- No communication when campus in a lockdown
- Police are slow to respond lack engagement



Q6. What is your perception of the strengths of the current safety and security program, what does the district do well? Select all that apply.

● Good communication on safety ...	67
● Secured buildings and classrooms	50
● Campus Police visibility	54
● Provision of emergency commu...	61
● Training	65
● Other	70



Q7. Are there immediate areas of concern that you feel needs to be addressed?

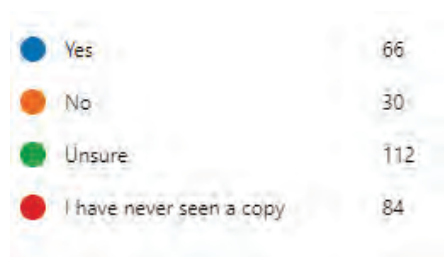
Responses to the open ended question included:

- Dispatch is a service and does not come directly to RCC Police. I see more RCC Police vehicles driving through Downtown Riverside than I see on campus.
- Ability to lock buildings from the inside is an issue
- Campus security meetings are not held regularly, are not promoted widely, and are not often held at times to encourage attendance.
- Faculty need to engage in use of lock bloks and locking doors at the end of class
- Dispatch not being directly connected to our police causes confusion as they do not know where our buildings are located.
- More police presence.
- Faculty need keys to rooms where they teach.
- Campus is very dark.
- More training needed to support incident response.
- All classrooms need a panic button.
- Would like a phone in the classroom
- Consider ID badges that support notification of need for help i.e., Centegix
- Classrooms are goldfish bowls at BLCIS on RCC campus, no area of concealment or hiding from an active shooter
- Provide training, which is currently not mandatory, improve communications when incidents are occurring

Q10. How often are you actively engaged in training, drills, education, and updates on safety and security?



Q13. Is a Campus/Building security plan developed, reviewed annually by administration, updated as needed and does it address shelter-in-place, threatened employee procedures, access procedures (anti-tailgating, etc.), threat recognition, duress alarm system, active shooter, lock down, etc. Select all answers that are applicable.



Q17. Are you aware of any protocol to summon law enforcement to the location of interest should a threat be suspected or identified?



Q21. Have you received any training or instructions on how to handle emergencies, such as active shooter situations or natural disasters?





Q23. Are there any areas where you feel access control is insufficient?

- The Admissions and Records area is a records office and currently has an open access door and hallway into the building. A sign indicates that only staff should enter, but that's not very secure as students have walked past the sign.
- Lock Blocks in the quad are not protection in case of active shooter or other campus threats.
- Students are not required to carry ID cards, and staff do not have photos on badges
- A weak point is the reception desk. If someone wanted, they could take her card key by force and work their way up every floor.
- Access cards are issued freely by administrators then faculty and staff allow others to use their cards, let others in without question and then those people prop doors open for others
- Admissions building is accessed through a swing door. There is nothing preventing a student from accessing the office of admissions and financial aid.
- We are an open campus and since faculty do not have universal keys, we do not have much control over locking and unlocking doors. We also have no place to call to report who is locked in, where, and how many, so there is no accountability.

Q26. Are there any areas that you feel security cameras should be installed that currently have no coverage?

- CSS building entrance (double sliding doors)
- Quad 1st and 2nd floors-could be placed in corners to scan. We have had student scuffles, and it would be nice to have a recording (or if they see the camera, they might not do the thing.)
- Inside the parking structure. My car was hit and run in there.
- All external cameras and hallways at the District - none of the cameras record
- I am not sure. Balancing privacy and security is difficult
- All over campus especially inside and outside building and parking lots. Someone needs to monitor the security cameras 24/7
- No buildings at RCC, other than those remodeled or built within the last year, have a working security camera system. Every time the talk of exterior security cameras comes up in meetings, nobody can decide what department will monitor them. Seems to make sense that the RCCD Police should manage this to easily streamline support for the victim or to deter people who may be up to no good.
- Everywhere on campus.
- Who would be in charge of monitoring them. this is unreasonable for a public place.
- I have heard that there are few if any cameras that are actively monitored. I do not know if that is true or not but that seems to be the common perception.
- Not sure where or if there are security cameras



Q30. Do you feel that classroom and office doors are equipped with appropriate measures to easily secure the space?



Q32. Are there any improvements that you would suggest for the current communication methods?

- Specialized training on how to secure during an emergency per each building and floor.
- Panic buttons are needed in the office spaces that provide direct services to students: Counseling, A&R and Financial Aid
- RCCD needs their own dispatch that is familiar with campus locations and is in immediate contact with RCCD police officers
- During our last active shooter drill, we received the alert through most methods (though some did not go through consistently). However, they did not give the 'all clear' signal through all the same methods.
- Cannot hear the emergency loudspeaker from inside the buildings.
- Specific details. We still have not received full details on the following incident: <https://www.pressenterprise.com/2023/11/02/juvenile-arrested-after-armed-robbery-reported-at-riverside-city-college/> from campus administration. It is unacceptable.
- Create a position dedicated to proper communication and risk management.
- We have seen MUCH improvement with how quickly alerts are sent to us, however, we are not given enough details about areas to avoid or the safety risk of what is happening. Being left uninformed can lead to unnecessary anxiety over what is happening, which can lead to people making poor decisions in an anxiety-ridden mindset.
- Lights or alarms on buildings letting everyone know that something is going on or to leave campus.
- Inform staff and students on campus in the event of an emergency when it is happening not after it has already taken place.

Q33. What changes or improvements would you recommend to enhance campus security?

75% of respondents provided comment in response to this question. Three areas of specific improvement trended including more visibility of the district police across the district campuses. Further engagement of district police to actively patrol campuses was commented by several respondents with some individuals specifically identifying presence during the hours of darkness as a request. Fifty (50) respondents requested the addition of video surveillance cameras, with several respondents further requesting that they be actively monitored. Eighteen (18) respondents reference access control, badging, and locked classrooms in their responses, illustrating a trend towards further controlling access to campus buildings through enhanced access control measures.

Further examples of respondents' improvement requests include:

- Building doors should be replaced to only allow entry with appropriate badge.



- Campus PA system, if a faculty member is in class teaching and their cell phone is put away, they will not be aware of an emergency text alert. an overall PA system that is designed to be heard over campus.
- Police presence (not parking services), timely response or information when an event happens (need to know only but do it more efficiently)
- More campus police visibility - used to see more patrolling in vehicles or even walking around on campus.
- The ability to block open view of the inside of the classrooms in the new BLCIS building
- Moderate presence of security and police, not just when incidents occur. Increased camera coverage. Increased blue phone coverage.
- Complete lockdown of buildings with access only to staff and students based on schedules
- Panic buttons in classroom
- Landline phones in every classroom
- Ability to lock classroom from inside, direct communication to emergency line from every classroom, regular and good training for emergencies and de-escalation



APPENDIX C - DISTRICT LEVEL PHYSICAL SECURITY FINDINGS



Physical security as defined by the *Facilities Physical Security Measures Guideline* (ASIS International, 2009, p.3) defines physical security as:

That part of security concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against a security incident.

The discipline of physical security consists of some combination of physical measures designed to protect assets (tangible, intangible, and mixed). Physical security measures should be considered in the context of their ability to deter and adversary, detect and attack, delay an attack, and deny an adversary access to the target. The concept of the four D's detect, delay, deter and defend should form the basis for all physical security projects (Physical Security Principles, ASIS International, p.16).

Physical security within education institutions is intended to provide a safe and secure learning and working environment for students, faculty, staff, and visitors. Within this section we detail the observation findings of the physical assessments and provide recommendations and suggestions for district level enhancement.

PHYSICAL SECURITY MECHANICAL

Brass Keys

Findings:

Robust brass key control issuance, retrieval, and management is an essential necessity of any security program. Maintaining awareness of brass key requests, documentation of issue, and provision of access to permitted spaces only is critical. Historically brass key management at education institutions has been challenging with keys often copied, shared, or not returned compromising security. Persons of responsibility turn over, along with antiquated means of documenting key requests, key type, date of issuance, and often a complete lack of retrieval process are common occurrences that are encountered. RCCD faces many of the identified issues regarding key management with no centralized electronic key management issuance and retrieval system in use. Local databases are administered by each college with no specific job function established that this activity falls under. Each campus has its own key request form that is submitted either manually (RCC and NC) or electronically (MVC) that requires subsequent approval through various layers of direct supervisor, departmental, and administrative review. All processes work and have merit, none are identical or standardized in workflow or documentation template used.

Figure 9 illustrates the Riverside College brass key request document with a two-layered form providing the employee with the top copy of information and a yellow hard copy kept on file by Facilities. Figure 10, illustrating the NC form is a single layer, with the form held on campus with no employee copy issued. Neither form is consistent in the information requested, including potential consequence of non-return of keys (there is no formalized board policy that is referenced regarding potential charging for non-return of keys, as indicated on the NC form). Both forms have good intent but are reflective of the lack of district driven standardization of process across RCCD.



In contrast, Figure 11 illustrates the electronic service desk key request form in use at MVC. This form indicates by display of all college names under the districts logo that it is a districtwide form, this is not the case, and its current use is local to MVC only. Upon submittal of the key request form automated workflow processes through before notification is provided to the requestor that their request is complete and keys ready for pick-up. There is no formal district key management policy and request and return procedure in place.

A major issue in the lack of retrieved keys was until recently upon an employee leaving employment of the district, exit interviews had occurred sparingly thus missing an opportunity for keys to be retrieved from those exiting. Absence of key retrieval has a major vulnerability impact on security, and many unaccounted-for districts brass keys remain with past employees that have left the district employment over the years. Rekeying of doors and buildings is costly and cannot be budgeted for each time a key is not returned, but it is the only means of eliminating this risk. Controlled key management should mitigate the frequency that lost keys occur, where possible electronic access control is encouraged to further reduce future brass key issuance needs to as few persons as possible.

The inconsistency in application of electrified access control across all campuses locations requires extensive use of brass keys to be issued and remain in circulation. The gaps in access control deployment influences the process of brass key issuance as many faculty members and staff require both keys and credentials to enter areas of authorized access. This further impacts the issuance of identification badges which at RCC is restricted to those who have security credentials only.

All locations are understood to be using restricted keyways reducing ability for easy duplication of keys at Minute Key Kiosks, hardware stores, internet off the shelf duplication machines, and at home use molding kits. Restricted keys are important as they are cut using patented key blanks that are not available on the open market, and every key can have a unique serialized code stamped into the metal. NC has recently (and continues to) implement the Assa Abloy Medeco secure keyways, this is a robust market leading option, other campuses use different keyways again demonstrating a lack of consistency in security measures approach. Standardizing on a single district keyway is recommended providing efficiency in the key management and hierarchy.

RIVERSIDE COMMUNITY COLLEGE DISTRICT
Please fill out form completely! KEY REQUEST KEY RETURN

FOR _____
Last First Phone _____

Email _____
Full/Part Time Dept _____

FULL TIME PART TIME

Campus _____ Department _____

BUILDING	ROOM NO.	KEY NUMBER

Department Approval _____ Key Received By _____ Date _____

Facilities Approval _____ Issued By _____ Date _____

To return key, tape key to back of hand copy.

FORM 1000 10/01/00

Figure 9 - Riverside College Key Request Form

**Brass Key – Key Card Access
Authorization & Return Receipt**

Identification/Proximity/Access Cards/Brass Keys
 Identification/Proximity/Access cards are issued to an individual and should never be lent or given to anyone else to use. The card access system logs via computer each time a card is presented for access. Lending or giving an access card to someone other than the authorized user may result in that access card being disabled and the user's card access privileges revoked.

Lost/Stolen Identification/Proximity/Access Cards/Brass Keys
 It is the responsibility of the employee issued the card to immediately notify the security department of a lost/stolen card. In the event the card is a proximity/access card, the card will be immediately disabled.

Property of RCCD-Norco
 All key cards (identification, proximity and access) and brass keys issued by RCCD-Norco (the District) are the property of the District. Upon termination of employment from the District, cards shall be returned to the Business Services department immediately. Failure to turn in a card may result in an employee being charged for a lost key card or brass key.

Brass Key/Key Card Access Assignment:

Employee Printed Name _____
 Department _____ Supervisor _____
 Employee Title _____

I understand and agree that any willful violation or violation of any part of this policy shall be considered full and sufficient cause for disciplinary action against me, which may include termination.

Employee Signature: _____ Date: _____

KEY RETURN RECORD:

Employee Printed Name _____ Signature _____
 Supervisor Signature _____ Date _____

Key(s) #: _____
 Card #: _____
 Issued/Rec'd by: _____

Figure 10 - NC – Key and Security Credential Request Form

The screenshot shows the RCCD (Riveridge Community College District) website interface. At the top, there are logos for Riverside Community College District, Norco College, and RCC. The main content area is titled 'Key Request - Digital Key Card'. Below the title, there is a 'Request Service' button. The page provides contact information for three locations: Maintenance Office, Operations Center, and Warehouse Building. A 'Details' section on the right shows a service ID of 1421, created on Thu 9/21/23 11:31 AM, and marked as 'Submitted' on Thu 9/21/23 11:42 AM. There are also sections for 'Attachments (0)' and a 'No file found' message.

Figure11 – MVC – Electronic Key and Security Credential Request Form



Recommendations:

Secure keyways, also known as restricted keyways, are essential to security program access control for several reasons:

- **Prevention of Unauthorized Duplicates:** Restricted keyways use unique key blanks and groove patterns that are not readily available. This makes it difficult for unauthorized individuals to duplicate keys.
- **Enhanced Security:** By controlling the distribution of key blanks, organizations can ensure that only authorized personnel can obtain and use keys. This adds an extra layer of security to protect sensitive areas.⁶
- **Access Control:** Secure keyways help manage who has access to specific areas. This is particularly important in environments where security is critical, such as campuses, critical infrastructure space and district offices.
- **Compliance:** Many industries have regulations requiring stringent access control measures. Using secure keyways helps organizations comply with these regulations and avoid potential fines or legal issues.
- **Audit and Accountability:** Secure keyways often come with key management systems that track who has access to which keys and when they were used. This helps in maintaining accountability and auditing access.

As identified, the district colleges currently use several different secure keyway solutions with no standardized solution. Performing a rekeying exercise of all campuses and administrative buildings to use one select solution is impractical and cost prohibitive. It is recommended that rather than aligning on a single district keyway at this time that each college standardize on their preferred solution and refresh all non-preferred solution keyways to the solution of choice through a phased upgrade program. Formalization of approved solutions should serve as governance for future building refreshes and new construction, ensuring that all keyways use the consistent solution at the specific college. The preferred solutions should be documented within district policy clearly stating the approved solutions per college with no deviation.

In contrast, it is recommended that there be a standardization of key issuance and retrieval process, formalized by district policy that directs use of a single electronic key management software solution. A single solution provides all district employees and faculty with a common platform, appearance, and process for key and security credential submittal request. The solution should support different workflows dependent upon nuances and needs of each college regarding their review and approval workflow. The digital request screen should appear the same to all, with workflow driven by college or administrative facility identifier. The current “Service Desk” process in use at MVC may be an option for scalability across RCCD, further investigation is encouraged to determine if this option can be applied across all campuses. There are alternate solutions available including Assa Abloy’s own SimpleK⁷ key management software platform that provides both key issuance and return workflow and key status management, in addition to supporting locksmith day-to-day key management activity. See Figure 12, for a snapshot of the automated key issuance agreement process.

⁶ [Key Control Best Practices Secure Access Management \(securityguards.org.uk\)](https://www.securityguards.org.uk)

⁷ [Key Control Software | SimpleK](#)



Figure12 - Assa Abloy SimpleK Key Control Software

Other features of Simple K include:

- Advanced tools for locksmithing and key control
- Manage all key systems (unlimited number of records)
- Robust import tools to bring current data into SimpleK
- Interactive floor plans
- Master key system design and expansion
- Key requests, approvals, issuances and returns workflow
- Cylinders and core pinning (verifies key interchange)
- Door-Key association visualization and rekeying solution
- Easily identify keys, access, and hardware on openings
- Visibility to audit trails and outstanding/overdue keys

Important to any potential physical key control system or software is the ability for interface/integrate with Active Directory and access control systems. This has been challenging historically and any potential selection and incorporation of a system such as SimpleK, InstaKey, Morse Watchman etc. should evaluate the interface/integration abilities of each. Benefits include push notifications through several means that an action is required.

Key aspects and benefits of integrating key control systems with access control systems:

- **Centralized Management:** Key control systems provide a centralized platform to manage all keys, ensuring that only authorized personnel have access to them. This helps in reducing the risk of lost or stolen keys.



- **Automated Tracking:** These systems use advanced technology to track the issuance and return of keys. This ensures that there is a clear audit trail of who accessed which keys and when.
- **Enhanced Security:** By integrating with access control systems, key control systems can enhance overall security. For example, if a key is not returned on time, the system can automatically deny a requestor access to certain areas when using SMART keys.
- **Alerts and Notifications:** Key control systems can send alerts and notifications to management if keys are not returned on time or if there are any unauthorized attempts to access keys.

Furthermore, management of brass keys should be supported by a formalized board policy. Policy should reference penal code that clearly illustrates the consequence of unauthorized duplication of keys; see CA Penal Code Section 469.

Any person who knowingly makes, duplicates, causes to be duplicated, or uses, or attempts to make, duplicate, cause to be duplicated, or use, or has in his possession any key to a building or other area owned, operated, or controlled by the State of California, any state agency, board, or commission, a county, city, or any public school or community college district without authorization from the person in charge of such building or area or his designated representative and with knowledge of the lack of such authorization is guilty of a misdemeanor.

Door Hardware

Findings:

Door locking hardware observed across the RCCD campuses and facilities as with the brass keys, consists of varying manufacturers, functions, and trim styles applied to spaces. There is no district standard Division 08 Windows and Doors employed to promote consistency of hardware installed based on space use needs across the District. Hardware manufactures Corbin Russwin (an Assa Abloy company), Assa Abloy, and Schlage Allegion, were the predominant hardware present. Door hardware appears to have been applied to openings on a case-by-case, project-by-project basis without direction from a district level regarding approved manufactures. Campus evolution over time, particularly at the RCC campus has resulted in several different manufacturer hardware types being installed. This is more prevalent at RCC simply due to the age of the campus and the continual development and addition of buildings, in contrast to MVC and NC which are less complex regarding the built environment evolution timeframe.

In addition to the varying hardware manufacture types observed, there are various types of door hardware functionality in use, including:

- Panic bar hardware with dogging capability.
 - Ability to retract the latch using a key cylinder or special tool, this capability when installed on access control openings allows for the security controls in place to be overrode, this should not be applied to access control openings.

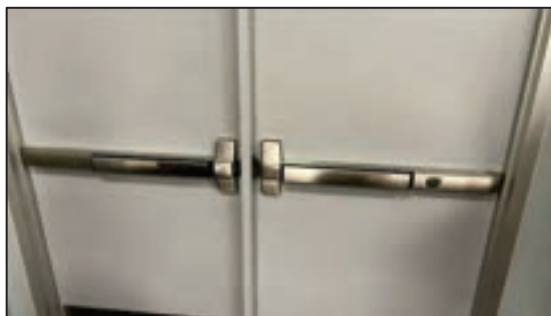


Figure 73 - Electrified panic bar with dogging – CAK Building (RCC)

- Panic bar hardware with no dogging capability.
 - No ability to retract the latch using a key cylinder or special tool, this trim style should be applied to access control openings where panic bars are installed.



Figure 84 - Electrified panic bar with no dogging – SAS Building (MVC)

- Mortise locksets.
 - Cassette style locksets installed into a pocket within the door, typically contain latch and deadbolt enclosed within the lock unit itself.

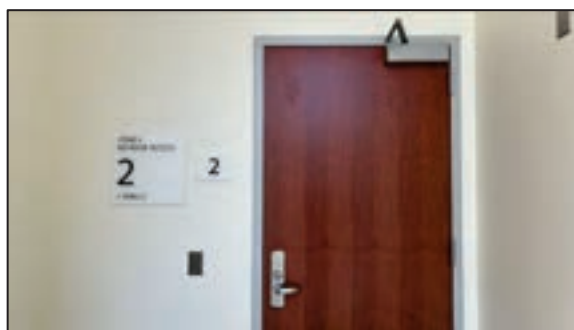


Figure 15 - Electrified mortise lockset – Nursing Building (RCC)

- Cylindrical locksets.
 - Simple installation through the door rather than within, latch is locked with a key and often can be retracted or secured from the interior using a key or thumb-turn/push button. These locksets do not include dead bolts.



Figure 96 - Cylindrical lockset with no internal locking option – SSV Building (NC)

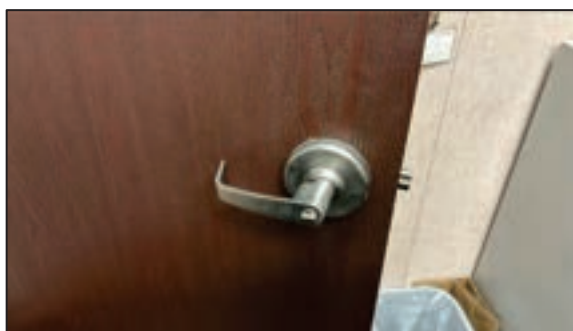


Figure 107 - Cylindrical lockset with pushbutton internal locking option – Portables A and B (NC)

- Traditional mechanical classroom function hardware with no internal locking capability i.e., key cylinder, push button etc.
 - Observed across the campuses, in the event of a lockdown the brass key holder must exit the space to secure the door from the public side if the door is operating in an unlocked state. This hardware function inherently could place a person or persons at risk in a lockdown event where they must lock the door. Policy could mandate that all classrooms function in a closed-door locked door state. Operational expectation of doors across colleges varies.



Figure 118 - Traditional classroom function interior locking hardware (Exterior) – HUM Building (NC)

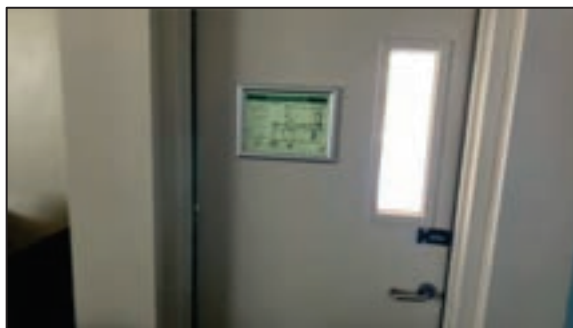


Figure 19 - Traditional classroom function interior locking hardware (Interior) – HUM Building (NC)

- Mechanical passage hardware at meeting rooms
 - No means of securing the door from either side, these locksets were observed on small meeting rooms.

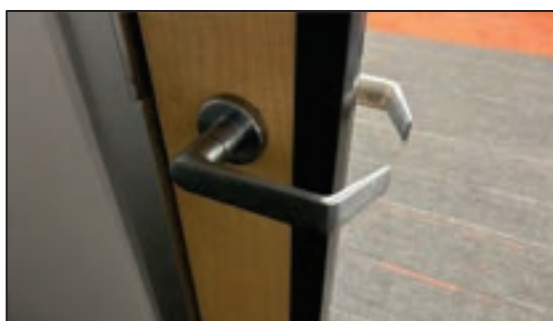


Figure 20 - Passage lockset – CAK Building (RCC)

Several types of door hardware were observed, but there does not appear to be a standard design approach governed by Division 08 that determines the correct door hardware function or trim components for each application. Door hardware is often overlooked in terms of its operational importance. The use of various hardware types has a wide-reaching impact on the ability for facilities and maintenance to manage and maintain them, as well as causing confusion for end users of the built environment regarding their expectations and utilization of door hardware. For example, a student in a classroom equipped with internal lockable hardware trim may assume that this is the norm across all campus classrooms. In the event of a lockdown, internal locking hardware requires a different response than external locking hardware. The inconsistent use of hardware across RCCD requires different understanding of use based on campus or administrative facility the end-user is occupying. A standardized application of door hardware, such as internal locking capability in all classrooms, would mitigate risk and potential liability issues, and support a simple train-and-educate approach for end-users to understand how to respond in the event of a lockdown across the District. The need to carry more than one access means, such as cards, and keys, for different hardware applications can be frustrating for end users, difficult to administer, and presents risk factors that can allow bad actors to exploit vulnerabilities in the inconsistent application of hardware.

A key observation regarding the inconsistent use of hardware across RCCD facilities is the disparate operational expectations of classroom doors at each campus. Operational understanding at each campus is:



Riverside City College: No operational expectation regarding door position or locking status when class is in session. Each individual space is secured at the preferred state that the instructor selects. Lock blocks are installed across campus, some doors remain unlocked, others locked, and many propped open during class.

Moreno Vally College: Doors are to be always in a locked state and closed when class is in session, the latch should be fully engaged, eliminating ingress. Lock blocks are installed at many classrooms but not permitted for doors to remain ajar for convenience of access.

Norco College: Doors are to be always in a locked state and closed when class is in session. The lock block is permitted for the door to rest in the jamb allowing free ingress and egress for convenience. In a lockdown the lock block is retracted and the door closes with positive latching restricting entry.

There is no formalized policy and subsequent protocol regarding door status in place across the district, in-turn no consequence for non-compliance is documented or enforceable.

Recommendations:

The RCCD security program can be strengthened by considering the following recommendation pertaining to both mechanical and electrified hardware, and operational expectations.

Mechanical Hardware

It is recommended that all occupants of classrooms and office spaces be able to quickly secure themselves in a lockdown using via an interior trim push-button or thumb-turn lever that indicates the door status. Training and review of door hardware functionality is recommended with all space users as part of employee annual training and space orientation for students at the beginning of each semester.

The following mechanical locksets are all manufactured by Corbin Russwin, similar locksets are available within the wider Assa Abloy range of products and are also available from Schlage. Each of the options provided provides ability for the door position status to be always known from the interior side of a space. Furthermore, the images illustrate the internal locking mechanisms specific to cylindrical and mortise locksets that allow ease of locking from the interior.



Figure 21 - CLX3300 Series with Status Indicator⁸

The CLX3300 Series cylindrical lock with status indicators delivers style, security, and enhanced privacy for both new construction and retrofit projects. Its six customizable indicator windows provide instant visibility of the door's lock status on the inside, outside, or both sides of the door. Engineered for easy installation in any setting, it features one-motion egress, non-handed design, and keyed functions. Exceeding Grade 1 standards, it is ideal for high-traffic restrooms, classrooms, and anywhere safety and privacy are crucial.

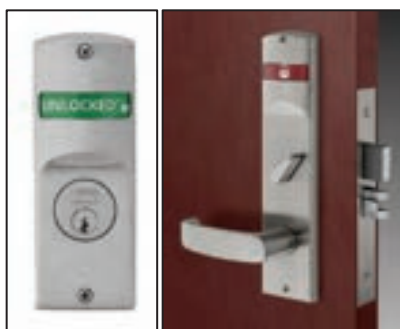


Figure 22 - ML2000 Indicator Series⁹

The ML2000 Series is a heavy-duty mortise lock designed for high-security applications. Enhance its functionality with our innovative Status Indicators, featuring a large, clear window that instantly displays whether a door is locked or unlocked. The versatile design seamlessly integrates with your existing hardware, providing an easy and effective way to improve access control and peace of mind.

⁸ [CLX3300 Series with Status Indicator | Corbin Russwin](#)

⁹ [ML2000 Indicator Series | Corbin Russwin](#)



Figure 23 - PED5000 Series Exit Device with Status Indicators¹⁰

Elevate your facility's safety and security with the PED5000 Series exit device with status indicators. Choose from three intuitive options to gain immediate visual confirmation of your door's status. The Active Dogging Indicator provides clear assurance that your door is secure, while the M48 Passive Dogging option offers a subtle visual cue. For enhanced classroom safety, the M47 Trim Status Indicator features a large display ideal for our Classroom Intruder function. With the PED5000 Series, you can rest assured that your occupants are protected.

It is recommended that the district standardize on a single door hardware manufacturer for all district buildings (or at minimum one manufacturer per campus) providing a more streamlined procurement and maintenance process than currently in place. Standardizing Division 08 to a single hardware manufacturer will reduce the effort needed to coordinate with different vendors when trouble shooting and procuring new hardware. This will provide the district with a stronger position for price negotiation as the potential product sales opportunity for a sole source supplier may significantly increase, supporting the district's ability to request a price reduction based on quantity procured ratio. It will also provide better service experience as the district account may be afforded a higher level of importance within the sole source provider who does not want to lose the account.

Electrified Hardware

Electrified door hardware provides numerous advantages for community colleges, significantly enhancing security, convenience, and efficiency. Some key benefits:

Enhanced Security: Electrified locks seamlessly integrate into a college's access control system, enabling better management of authorized access to specific areas.

Convenience: Electrified hardware allows for remote door control, reducing reliance on physical keys and enabling swift lockdowns or access adjustments.

Cost-Effectiveness: Despite the initial investment, electrified door hardware invariably yields long-term savings by minimizing the need for key replacements and enabling more streamlined security management.

¹⁰ [PED5000 Series | Corbin Russwin](#)



Accessibility: Automated electrified doors promote compliance with the Americans with Disabilities Act (ADA), rendering entrances more accessible to all students and staff.

Hygiene: Touchless entry options play a vital role in unequivocally curbing the spread of germs, particularly advantageous in a community college environment where multiple individuals utilize the same facilities.

As with the mechanical locksets, the following electrified locksets are all manufactured by Corbin Russwin, similar locksets are available within the wider Assa Abloy range of products and available by Schlage.

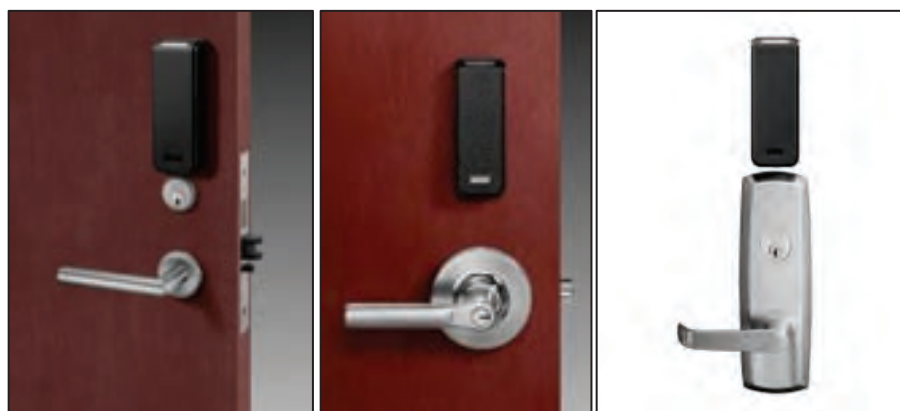


Figure 24 - Electrified Hardware - SN210 ML2000 Series, SN210 CLX3300 Series and SN210 ED5200 Series¹¹

The Corbin Russwin electrified hardware illustrated in Figure 24, illustrates the SN210-ML2000 Series (mortise lockset), SN210-CLX3300 Series (cylindrical lockset), and the SN210 ED5200 Series (emergency panic bar exterior escutcheon). All three and similar by others will seamlessly integrate with the existing Software House CCure 900 access control system (and others). Locksets support multiple communication types including traditional Wiegand and newer Open Supervised Device Protocol (OSDP), providing continuously monitored end-to-end wiring, protecting against tampering and “man in the middle” attacks.

Features and Benefits of the electrified hardware include:

- Open architecture platform
- Integrated design incorporates all access control components, including card reader, door position switch, and request to exit monitoring sensors
- Lockdown capable
- Multiple credential technologies, offering easy migration to higher security credentials or consolidation of mixed credentials
- Supports PIN only and dual authentication requirements
- Compatibility with all popular access control systems
- Ability to secure areas immediately from central security system

¹¹ [SN210 ED5200 Series | Corbin Russwin](#)



- Reduced installation time and costs; improved reliability
- Field configurable to fail-safe or fail-secure
- Operates from 12-24VDC, offering greater flexibility in system design
- Innovative actuator design provides superior reliability

Electrified hardware should be upgraded and implemented as part of any new existing building refresh program or new construction project. Division 28 Electronic Safety and Security Standards should govern application of electrified hardware, these should be developed in conjunction with reference to Division 08.

Operational Expectations

Operational expectation of classroom doors is affected by the culture, community, and end-user expectations at each campus and administrative facility. The districtwide closed door, locked door approach when in class is implemented most robustly at MVC. It is recommended that all classroom doors always remain in a locked state. Policy should be created that defines the expected operational state per campus, and consequential protocol created that supports enforcement of the approved operational states. Lack of protocol and follow-through where non-compliance is identified renders the initial policy worthless.

Lock Bloks

The lock blok is a common and inexpensive device that allows for doors to function in a closed lock state without positive latching, allowing free ingress and convenience, but immediate closure and positive latching upon retraction of the blok. The lock blok is typically used on out-swinging doors affixed to the door itself with the blok protruding into the door jamb when in use. In-swinging doors can benefit from the device by affixing it to the door frame, the same scenario of closure occurs when retracting the blok.

The lock blok is widely used across the three RCCD campuses and is encouraged to continue to be used specifically on doors with mechanical hardware that function in a locked state. Application on doors that are egress only should not occur with those openings remaining closed and locked with no free ingress. Use of lock bloks on access control openings was observed and can be challenging when an access control system is fully managed and alarm events responded to. Typical use of a lock blok on an access control opening would provide a 'door-held' alarm event after a predetermined period, if used. Use of lock bloks at access control openings requires review of systems programming to mask door position status when used. The district is currently not operating with any robust management of the access control systems. Programming considerations are required if lock bloks are to be used at controlled entries in the future.

Lock blok use should be governed by security standards and district policy supported by consequence for misuse.

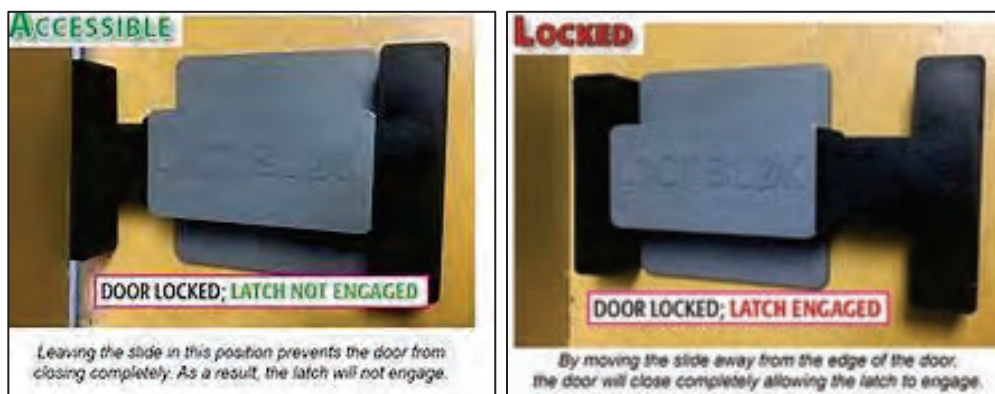


Figure 25 - Lock Blok Use Position Status



Figure 26 - Lock Blok Strap

A number of lock blok straps were observed across campuses, these are not recommended for use as they require the door to be opened for strap removal and door closure for positive latching.

Glazing and Door Treatments

Glazing is an important factor in providing students with visual connectivity to their place of learning which can be beneficial for both mental health and wellness. Use of high performing glass can manage glare from the sun, deflect UV transmission, support heat and draft management maintaining a comfortable learning environment, and support noise reduction when high STC (Sound Transmission Class) glazing is used. Additionally glazing supports the CPTED natural surveillance and eyes-on-activity principle which can increase safety and security with increased visibility of activity and supervision.

Findings:

Various types of glazing and door window vision panel treatments are in use across RCCD, the typical application of window treatments is from the perspective or reducing sun glare into classrooms, rather than from the restriction of public visibility for safety and security purposes. This is not an uncommon finding amongst community colleges, with

continual evolution of campuses and building expansions occurring over many years (prior to safety and security awareness being as prevalent as it is today).

General observation found no consistency of application of window treatments across campuses. It is assumed that window treatments are applied on a project-by-project basis with the final solution approved by building end-user stakeholders at the time of construction. Design standards have been requested but not received or referenced during stakeholder interviews (it is assumed that they do not exist). Several locations have inoperable window treatments, challenges with end-user reachability, and a need for repair, these individual observations are detailed within the Appendix F reports.

A selection of window treatments observed include:



Figure 27 - NC CSS Building

Reflective film with no ballistic protective measures. Film performance is reversed when lights are turned on, visibility into the area during darkness is unrestricted when interior lights are in use. Film requires maintenance review within the canteen area where the film is peeling from the glazing. Automatic window blinds provide an initial layer of visibility restriction when activated.

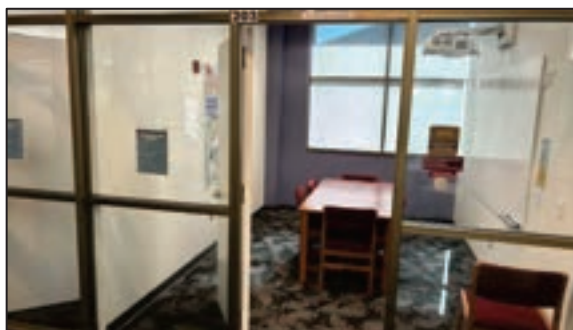


Figure 28 - NC LIBR Building

No internal window treatments to restrict visibility at the private learning spaces. This impacts potential hiding locations for occupants within the library space should a lockdown be initiated. Occupants of these offices are required to congregate in a shelter-in-place location at the rear of the library during a lockdown.



Figure 29 - NC Presidents Office

Visibility into the President’s Office is excellent during the hours of daylight. During hours of darkness visibility into the space is reversed and the occupants fully exposed to external visibility. The glazing has no ballistic protective measures applied to it.



Figure 12 - RCC Facilities Building

Window blinds are lowered at the Facilities Department restricting visibility from the public side in. Glazing is old and illustrates the different levels of glazing in use across the campus. Reflective film is not applied to the glazing.

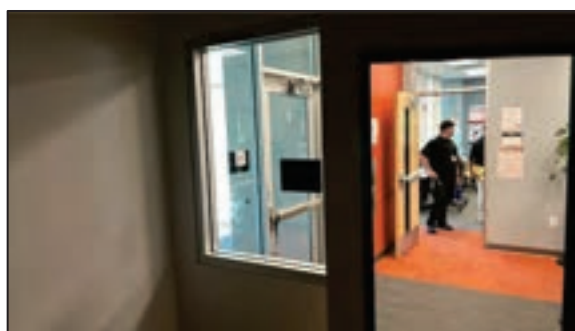


Figure 131 - RCC CAK Building

No internal window treatments to restrict visibility at the private learning spaces. This impacts on potential hiding locations for occupants within the CAK space should lockdown be initiated.

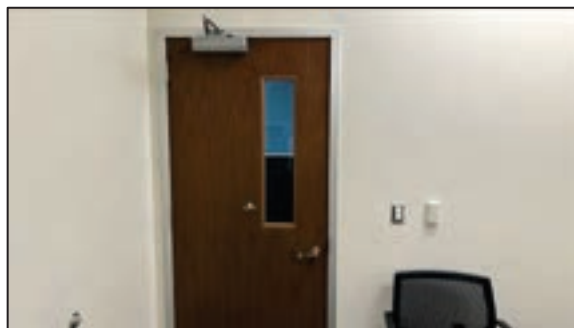


Figure 32 - MVC Counseling Offices

Self-made door window vision panels were observed applied to the Counselling Offices at MVC. Concerns were raised by the Facilities Team at MVC who have had to respond to panic button activations with no ability to look into all offices as several have the vision panel completely obscured. No coordination with the Fire Marshal appears to have occurred to identify best practice for provision of visibility into office spaces. Door window vision panel treatments at office spaces across RCCD vary by building, application, and end user choice.



Figure 33 - Culinary Arts Academy

Floor to ceiling glazing with restrictive visibility frosted film is applied to the first-floor windows at the Culinary Arts Center. It is understood that there is no ballistic protective elements to the film. The glazing is adjacent to the public sidewalk and University Ave., which experiences heavy traffic throughout the day and night. Incidents involving the brandishing of firearms have occurred in the immediate vicinity as shared during stakeholder interviews.

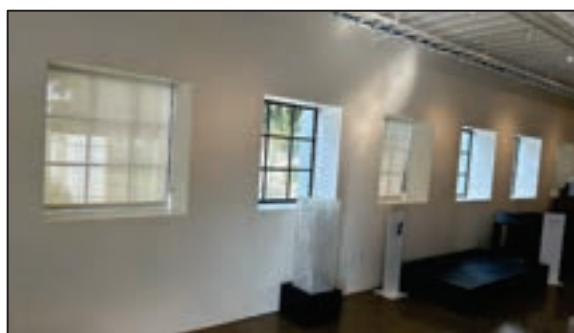


Figure 34 - Center for Social Justice and Civil Liberties



Broken glazing has occurred at the Center for Social Justice and Civil Liberties while the building was occupied during an event. The ground level windows are a comfortable height for peering in from the public side. Window treatments when lowered do restrict some but not all visibility when lights are on. During hours of darkness the opaque material of the blinds does not obscure vision in.

Recommendations:

Modern education institution-built environment conditions must consider glazing protective measures as a critical component of the safety and security program. The threat of an active shooter incident occurring remains statistically low, however the protection of students, faculty, and staff is paramount and can be supported by intelligently designed and fortified windows.

¹²In 2022, the glass industry came together and published ASTM F3561, Standard Test Method for Forced-Entry-Resistance of Fenestration Systems After Simulated Active Shooter Attack. This new standard is designed to serve as the minimum accepted standard for security glazing in schools. When applied correctly, the windows and doors can significantly slow down the attacker during an active shooter event. This allows more time for schools to enact emergency plans and for first responders to arrive.

It is important to note that ASTM F3561 is an enhanced forced entry test – not a bullet resistance test. If bullet resistance is needed, glass tested to UL 752, Standard for Bullet Resisting Equipment, must be used.

Selection of glazing protective measures can be affected by risk appetite, cost impact, physical appearance, and built environment conditions amongst other things. Different types of glazing resistance levels may affect the glazing selection when considering security intent.

The appropriate glazing penetration resistance should be determined based on the below descriptions of levels of resistance: Basic, Enhanced, Ballistic Protection, Forced Entry, Enhanced Forced Entry, Multiple Forced Entry Assault (Ballistics + Forced Entry) and Blast Mitigation.

¹³**Basic:** The basic level of safety glazing is based on human impact forces and glass containment upon breakage. Often written into building codes, the intent is to ensure the glass has enough strength to withstand accidental impact with the glass and has requirements that glass fragments be contained to avoid injury. The products rated for this category are recommended for situations such as slowing immediate entry through glass and reducing the ability of someone to reach through an opening to release a door handle. Products such as laminated glazing or surface-applied safety films are readily available to meet applicable test standards.

¹² [Why Glass Safety Matters in Educational Settings - Safe Glass for Schools](#)

¹³ [FB71-21 School Security Glazing \(glass.org\)](#)



Enhanced: Burglary resistant glazing can be a deterrent to smash-and-grab crimes involving the use of hands, elbows, fists, and general burglary tools such as a hammer. Products in this category are intended to deter vandalism such as breaking into a display case or entering the building and fleeing.

Ballistic Protection: Bullet-resistant (BR) glazing is designed to resist penetration from a variety of firearm ammunitions. Several examples of bullet resistant laminated glazing include all-glass laminates, glass clad polycarbonate laminates, glass laminates containing other rigid polymers, laminated polycarbonates, and glass/exposed plastic laminates (exposed polycarbonate or PET). Bullet-resistant glazing provides an improved safety barrier against bullets and related flying glass or plastic fragments (spall or splinters). Bullet resistant glass has weight considerations that could affect structural loads when employed. This is a cost consideration that affects not just the window, but the supporting structure.

Forced Entry: Forced entry (FE) resistant glazing is designed to increase the amount of time required to gain entry. This additional time is intended to allow for the enactment of lockdown protocols. These products may be used in areas with high risk of prolonged attack or in critical areas such as entry vestibules. Forced entry resistant glazing should meet the criteria above and resist penetration from hand-held or hand-thrown objects such as hammers, crowbars, bats, knives, bricks, and rocks.

Enhanced Forced Entry: Products in this category are intended to meet the requirements for forced entry resistant glazing after being weakened by ballistic assault. They are not designed for ballistic classification; thus, the bullets may penetrate the glazing. Enhanced forced entry testing can include shooting through the glass to weaken it followed by physical impact with various weapons. The glazing classification would carry an indication of the type of ballistic assault used along with a forced entry classification. The goal is to resist entry for an adequate amount of time to allow for the arrival of emergency response personnel.

Multiple Forced Entry Assault (Ballistics + Forced Entry): Products in this category are designed to combine the resistance of ballistics classified laminates with additional resistance to forced entry. Testing for these glazing systems involves weakening the sample by ballistic assault but not allowing the bullets to penetrate. The glazing is then tested to withstand physical impact and attack with various weapons. This glazing would carry a ballistic and forced entry classification and would be used in very high-risk areas, where intruders may be armed with guns.

Blast Resistance: Blast-resistant glazing can reduce injury from flying glass resulting from direct blast shock waves (over-pressures). When properly designed, framed, and anchored, blast-resistant glazing is capable of maintaining the integrity of the building envelope following an explosion and reducing interior damage. Blast-resistant glazing may offer some level of burglary or forced entry resistance but without testing to burglary or forced entry standards, how much resistance is not quantifiable. Also, this glazing is not typically bullet-resistant without being tested to a ballistic threat level.

Glazing protective measures described can vary significantly and application influenced by space functionality, frequency of use, local crime statistics, event staffing, and culture. As with security electronics, an RCCD physical security design guideline and standard is recommended providing direction and guidance to all future design and construction projects that a minimum baseline expectation is required driven by space use. Simple selection of a specific glazing type alone is not sufficient, review and analysis of other building materials in conjunction with glazing



is critical to a robust protective envelope being established. Appropriate wall materials are required if the intent is to prevent projectile penetration in the event of an active shooter. Future district glazing considerations should consider the following security selection quick reference summary table.

Security Selection	Test Standard	Security Level of the Selection*		
		Low	Medium	High
Basic Safety Glazing	ANSI Z97.1	Class B		Class A
	CPSC	Cat I		Cat II
	CAN CGSB	Class B		Class A
	ASTM F3006/F3007	0.75 m Cat 2	3.66 m Cat 3	3.66 m Cat 2
Enhanced	UL 972	Std – 10 ft	Ind/Outdoor	High Energy (40 ft)
	ASTM E2395	L1	L3	L5
	ASTM F1233	1.0	1.1	1.2
Forced Entry	ASTM F1233	1.4	2.3	5.0
	ASTM F3038 – mob with hand tools	5 min	15 min	30 min
Enhanced Forced Entry	ASTM F1233 Annex A2	3 shots with 9 mm handgun; Class 1.4	3 shots with .357 Magnum; Class 2.3	3 shots with .44 Magnum; Class 5.0
Ballistic Protection (Handguns)	UL 752	1 (9 mm handgun)	2 (.357 Magnum)	3 (.44 Magnum)
	ASTM F1233	HG3 (9 mm handgun)	HG2 (.357 Magnum)	HG4 (.44 Magnum)
Multiple Forced Entry Assault (Ballistics + Forced Entry)	ASTM F1233	HG1/R1-1.4	HG2/R2-2.3	HG4/R3-5.0
Blast Resistance	ASTM F1642/F2912	H3	H2	H1

*This is not meant to be all-inclusive; there are levels existing outside of this table.

Table 10 - Security Selection Quick Reference Summary Table

The *Department of Homeland Security: Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings*, provides general design guidelines for windows and glazing including some of the listed that the district may consider for adoption within its standards:

- Orient glazing perpendicular to the primary façade to reduce exposure to blast and projectiles.
- Place windows away from doors so that, if the windows are broken, the door cannot be unlocked.
- In areas requiring high security, minimize the number and size of windows in a façade. The amount of blast entering a space is directly proportional to the amount of opening on the façade.
- Consider using burglary and ballistic-resistant glazing in high-risk areas.

- Consider using laminated glass in place of conventional glass.
- Consider window safety laminate (such as mylar) or another fragment retention film over glazing (professionally installed) to reduce fragmentation.
- Place horizontal windows 6 feet above the finished floor to limit entry.
- Consider using steel window frames securely fastened or cement grouted to the surrounding structure.
- Minimize interior glazing in high-risk areas (e.g., lobbies, loading docks).

In addition to glazing types, security film is another method of making windows and glass doors safer. Security film coats the glass window on one side, helps prevent the spread of glass fragments when the window is shattered and slows the velocity of the shards should the glass fail. Security film, also known as fragment retention film, is particularly useful for existing windows, as it can be applied to the outside of the window itself. Like ballistic glass, security film can also slow down an active shooter, which allows people to get out of buildings and provides first responders time to respond to a threat. Security film can also mitigate the effects of an explosion. Should a bomb explode in or near a campus, security film on windows and glass doors can help mitigate the effects in one of two ways; either the film will prevent the glass from fully shattering, or it will help slow down the fragmentation, mitigating further injury. Security film can also protect against burglary due to windows shattering. Leading market providers include Safe Haven Defense¹⁴ and Clear Armor¹⁵.

It is recommended that the district meet with District Police and the local Fire Department when making decisions about physical security associated with openings i.e., doors and windows. This can ensure that all physical security changes adhere to building and fire code and do not impede the accessibility of emergency services if called upon to respond to an incident.

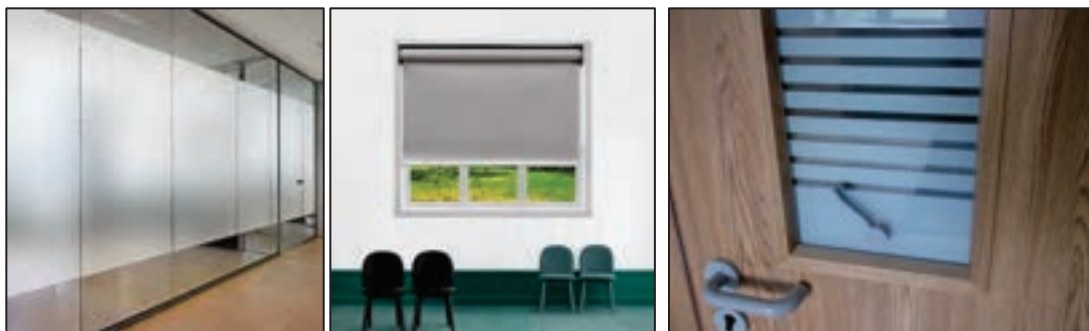


Figure 35 - Interior Window Treatments

As with the glazing considerations, internal window treatments should be standardized based on space functionality. Internal applications are primarily providing privacy from external viewing. Consideration to window treatment intent should be given thought prior to installation, i.e., if frosted film is intended to prevent visibility of a space occupation, this is not going to occur with window frosting which is intended as a privacy barrier and not to 100% obscure

¹⁴ [Safe Haven Defense - You Can Shoot Out But They Can't Shoot In | Safe Haven Defense](#)

¹⁵ [Bulletproof Glass - Clear-Armor | Best Armored Laminates](#)



identification of space occupation (silhouettes still visible). Ease of access, and use is important with blind drawstrings located above 6' presenting height restriction challenges. Regular testing should occur, and repair of any window treatments identified as inoperable or needing attention managed through a service ticketing system.

Vehicle Controls and Perimeter Protection

Findings:

Community colleges by their very nature strive to be welcoming and open spaces with a purpose that far exceeds the core learning services provided. RCCD is no different and its campuses and other facilities provide community services that encourages the use of their facilities not just by students but by the wider public i.e., Culinary Arts Academy open Cafe. Perimeter protection from a physical perspective (gates, barriers, and fences etc.) is minimal in use across the three college campuses which all have varying levels of physical perimeter protection in place. The downtown Riverside facilities, with exception of the secured maintenance yard between the District Office and the Henry W. and Alice Edna Coil School for the Arts, rely on the building exteriors themselves as the initial layer of security and perimeter controls are minimal in presence. As with the college campuses these buildings are open to public use and the local community are welcomed and encouraged to use the spaces.

Access control, staffed entrances, and District Police Parking Staff presence does provide opportunity to show a physical presence of security staffing. Patrols however are infrequent. This physical presence alone is not satisfactory to allay the concerns of downtown facility staff and faculty who frequently encounter interaction with homeless and agitated members of the local community. Furthermore, perimeter protection measures are inconsistent in deployment across the three downtown facilities that all reside on the same two blocks. For example, the District Office can be secured immediately via a remote switch and electrified front door hardware, the Center for Social Justice and Civil Liberties front door located less than 50' from the District office cannot be automatically secured and relies upon physical locking by staff. The lack of consistency and standardization regarding security measures application creates risk and vulnerability that could be avoided with security standards serving and defining minimum baseline security conditions. Technology such as video surveillance is underutilized with no localized streaming of video to internal viewing monitors and key stakeholder's workstations/laptops, failing to support and strengthen the security program with eyes-on-activity.

Vehicle Controls

College campus perimeter protection is porous across all three campuses with unrestricted pedestrian and vehicle access available. Compartmentalization of vehicle access onto campuses with existing security measures can be best achieved at RCC and MVC with swing-arm barriers installed that when closed and locked reduce vehicle access into parking lots, and into access lanes. There is an operational understanding at MVC that the swing arm barriers are closed and locked each night by Campus Police. At the time of assessment barriers did not appear to be secured at any point. Barriers at RCC do not get secured and remain permanently open with no access restrictions in operation. NC has no vehicle perimeter protection measures in use other than removable bollards at the service road adjacent to the Operations Center. NC has the largest parking lot space and a single point of entry into the campus via Third St. that would support the easiest compartmentalization, restriction, and control of traffic across all three campuses using vehicle barriers such as swing arm barriers.



Figure 146 - Unsecured Swing Arm Barrier (MVC Portables)

Figure 36 illustrates an example of an unsecured swing arm barrier at MVC that remains open and always unlocked for convenience despite mobile A-frame signage indicating that the road is closed. The roadway is free access from the adjacent parking lot into a classroom area presenting risk that can easily be mitigated with closure and securing of the swing arm barrier.



Figure 157 - Speed bump (RCC Warehouse)

Speed bumps are deployed across the campuses but sparingly. Speed cushions are not used across any campuses restricting general vehicle speeds but allowing buses and first responder units to easily traverse. Supporting speed restriction signage is minimal in deployment with no consistency in speed amount, signage sizing, font, and text deployed.



Figure 168 - Parking Garage Gates (RCC)



Figure 179 - Parking Garage Gates (District Office)

Parking garage gates were observed at both RCC and the District Office. RCC garage gates are mechanical and typically remain open 24/7, the gates are located at the lower entrance, with an upper entrance devoid of any vehicle control measures to support restriction of parking garage vehicle activity. An electrified gate at the District Office parking garage is manually closed each evening and reopened daily to restrict vehicle access after a predetermined time. Free egress of vehicles is always available with vehicle loops embedded in the floor triggering the gate to unlock when activated by a vehicle presence. Circular speed bumps are present in the parking garages with intent to reduce vehicle speeds between 2-10 miles per hour. Vehicles were observed by passing these speed bumps at the RCC parking garage for convenience and speed of ingress and egress.



Figure 40 - Third St. (NC)

An observation of significant safety and security risk is the NC Third St. main entrance access road. As detailed within the individual findings report, the shared access to JFK Middle College High School and NC is a 1,000ft + multi-laned road with minimal physical roadway speed control measures. Vehicles can easily hit speeds more than 65 miles-per-hour from point of entry onto Third St. up to the Sports Complex. Speed control signage, raised crosswalk, speed cushions, roadway painted signage are all traffic calming measures that are not used to support speed restrictions. It should be noted that this area was specifically brought to the assessment teams' attention by a member of faculty while the team was observing the area. It was shared that several near misses of pedestrian and vehicle collisions have occurred at the crosswalk area. There is no delineation of school and college traffic points of entry, with minimal directional signage used to support better traffic control.

Fencing and Gates

Application of fencing and gates across campuses was observed as intentional in their use at the facilities/operations and maintenance departments and the Early Childhood Education Centers (ECEC) at RCC and MVC. Fence and gate heights and material varied, with chain-link most typical, and decorative fencing observed at the Aquatics Center at RCC.

Securing each campus with perimeter fencing is unrealistic and not conducive to the intent and purpose of community college availability for public access. Use of fencing should be more focused providing deterrent to bad actors and delineating space that is not freely accessible without authorization. Below are our fence observations:

Wooden lodge pole rail fencing at NC adjacent to the horse trail is rotting and requires replacement. There is potential that the fence could collapse if leaned against by a person leaning against it, causing injury. Cross beams of the fencing are reusable, but posts require replacement at several locations along the fence line.



Figure 41 - Wooden lodge pole rail fence line with rotting posts at NC

The chain-link fencing at the ECEC at RCC provides no reduction in visibility from the public sidewalk and is easily scalable as its height is approximately 4'. Inconsistent height of the fence line further supports ease of unauthorized access (a frequent occurrence at RCC) as the 6' tall vinyl fencing provides support for climbing over the chain-link fence. The fence line at the RCC ECEC fails to restrict both visibility of activity and entry into the playground and is an item of concern for ECEC staff.



Figure 42 - Fencing at the ECEC at RCC Playground

Fencing at the MVC ECEC is similar in application to that found at the RCC campus. A combination of vinyl fencing, and chain-link fencing and gates fail to reduce visibility of the childcare playground as the adjacent sidewalks are elevated. Furthermore, side access gates at the playground were found unlocked providing both unrestricted entry for both authorized and unauthorized persons, and gates could easily be passed through by children if they were intent on running away. Gates are not monitored, providing staff with notification of gate status i.e., closed, or open.



Figure 183 - Fencing and Gates at ECEC MVC Playground

Decorative fencing, although visually appealing, provides ease of scaling at the RCC swimming pool area with a flat top rail that supports a bad actors ability to pull themselves up and over the top. The height of the fencing also fails to provide any deterrent. A lack of video surveillance does not permit the use of technology and video analytics to proactively notify activity within a specific area (i.e., fence line) and trigger an appropriate response protocol.

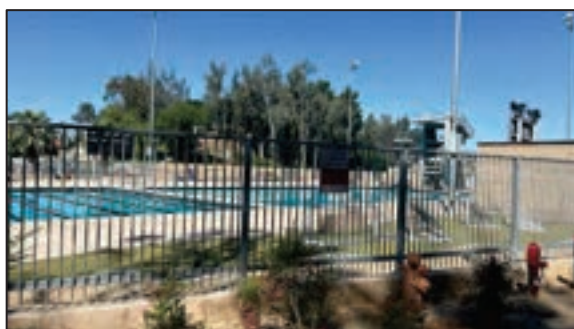


Figure 194 - Decorative Fencing at RCC Swimming Pool

Other observations made included chain-link roller gates with gaps below the gate that provide ease of access by crawling underneath (i.e., both gates at the NC Operations Center and RCC Facilities Yard), damaged fence lines at RCC above the Facilities Yard and at the ECEC parking lot, gaps in level one fencing at the parking garage downtown creating entry vulnerability, and plant overgrowth protruding into fencing at NC Sports Complex. All are examples of additional issues with existing fencing.



Figure 205 - Overgrowth protruding through the fence at NC Sports Complex



Recommendations:

Vehicle Controls

It is recommended that the district take a holistic approach to reviewing and refreshing, adjusting, implementing traffic control, and calming measures. Traffic calming is a strategy of CPTED and can contribute to CPTED principles:

- **Natural Surveillance:** Slower traffic allows campus users and pedestrians to observe their surroundings more effectively.
- **Territorial Reinforcement:** A calmer environment fosters a sense of ownership and community engagement.
- **Access Control:** By reducing traffic speed and volume, potential offenders have less opportunity to access areas unnoticed.
- **Activity Support:** A safer environment encourages people to use public spaces, increasing natural surveillance.
- **Maintenance:** Traffic calming measures can help preserve the overall appearance and condition of a campus.

Suggested physical traffic controls measures for consideration include:

Speed Signs – Display of permitted speed allowable, recommend 15 MPH (refer to CVC for guidance). Signage should be easily visible to approaching vehicles, easy to read and placed consistently throughout campuses where vehicles access.

Guide Signs – Display of physical signage that indicates the traffic flow or areas of specific vehicle parking locations. Signage should be easily visible to approaching vehicles, easy to read and placed at appropriate locations with specific directional traffic flow or areas of parking for certain vehicle types.

Pavement Markings – Guidance markings that communicate directional information to approaching vehicles. For example, pavement markings providing vehicle access direction at Third St. (NC) would support the traffic management required for safe vehicle entry at JFK Middle College High School. Pavement markings support reinforcement of accessibility for vehicles to areas that they require access to.

Speed Cushions - Speed cushions are either speed humps or speed tables that include wheel cutouts to allow large vehicles to pass unaffected, while reducing passenger car speeds. They can be offset to allow unimpeded passage by emergency vehicles and are typically used on key emergency response routes. Speed cushions extend across one direction of travel from the centerline, with longitudinal gap provided to allow wide wheelbase vehicles to avoid going over the hump. Third St. at NC should be considered a prime location for use of speed cushions, liaison with emergency response officials is recommended prior to any action that results in installation.



Figure 216 - Speed Cushions

Speed Bumps – speed bumps are typically raised 2” or 3” above the roadway and are no more than 12” wide. Travel over them at speed delivers an abrupt disturbance that cannot be ignored and typically a slow speed is required to travel over them comfortably without experiencing an abrupt “thud” impact. Placement of speed bumps within parking lots and access roads would support restricted speed intent.



Figure 227 - Speed Bump

Raised Crosswalk - Raised pedestrian crosswalks serve as traffic calming measures by extending the sidewalk across the road and bringing motor vehicles to the pedestrian level. Raised crosswalks also improve accessibility by allowing a pedestrian to cross at a constant grade without the need for a curb ramp and makes the pedestrian more visible to approaching motorists. Roadways are not the only places traffic calming devices can be useful. Raised crosswalks can be used in school parking lots to slow traffic and more safely allow pedestrians to cross the parking lots. When used,

care must be taken to accommodate drainage in the parking lot and to prevent water from pooling.¹⁶ There are several locations across RCCD campuses where raised crosswalks would support reduction in vehicle speed. Again, most predominantly at Third St. NC, as well as at areas already defined with pavement crosswalks at RCC and MVC. Evaluation of appropriate solutions is encouraged as development of existing pavement only crosswalks to raised crosswalks may be adequate to provide speed controls at specific locations.



Figure 238 - Raised Crosswalk

Bollards - use of K-rated vehicle bollards or engineered concrete planters, furniture, or other obstructions which can prevent a vehicle traveling at speed from impacting crowds or buildings at key locations may have their place in maintaining safety and security on a case-by case basis.

Bollards may be considered at locations that are:

- Areas of large student congregation.
- Areas adjacent to industrial vehicle pathways.
- Building entrances with direct path of access to vehicles.
- Walkways or pathways adjacent to vehicle pathways long and straight enough to allow a vehicle to reach speeds more than 30 miles per hour.
- Campus entry points, allowing for closure to unauthorized vehicles, as necessary.

A specific area identified that may benefit from a risk reduction perspective by installation of bollards is the bus drop-off and pick-up area in front of the Welcome Center at MVC. The main campus entry from College Drive provides unrestricted accessibility onto the sidewalk and pedestrian pavement area directly from the roadway. There is no physical barrier or deterrent currently in place. Operational needs may require removable bollards to be installed if considered. Lack of signage, speed cushions or raised crosswalk fail to support traffic calming. It is recommended that

¹⁶ [SRTS Guide: Raised Pedestrian Crosswalks \(saferoutesinfo.org\)](https://saferoutesinfo.org)



the district review any future vehicle bollard Installation from an individual campus operational impact perspective, with focus on identifying how to implement vehicle control measures while minimizing impact on maintenance and operations accessibility.

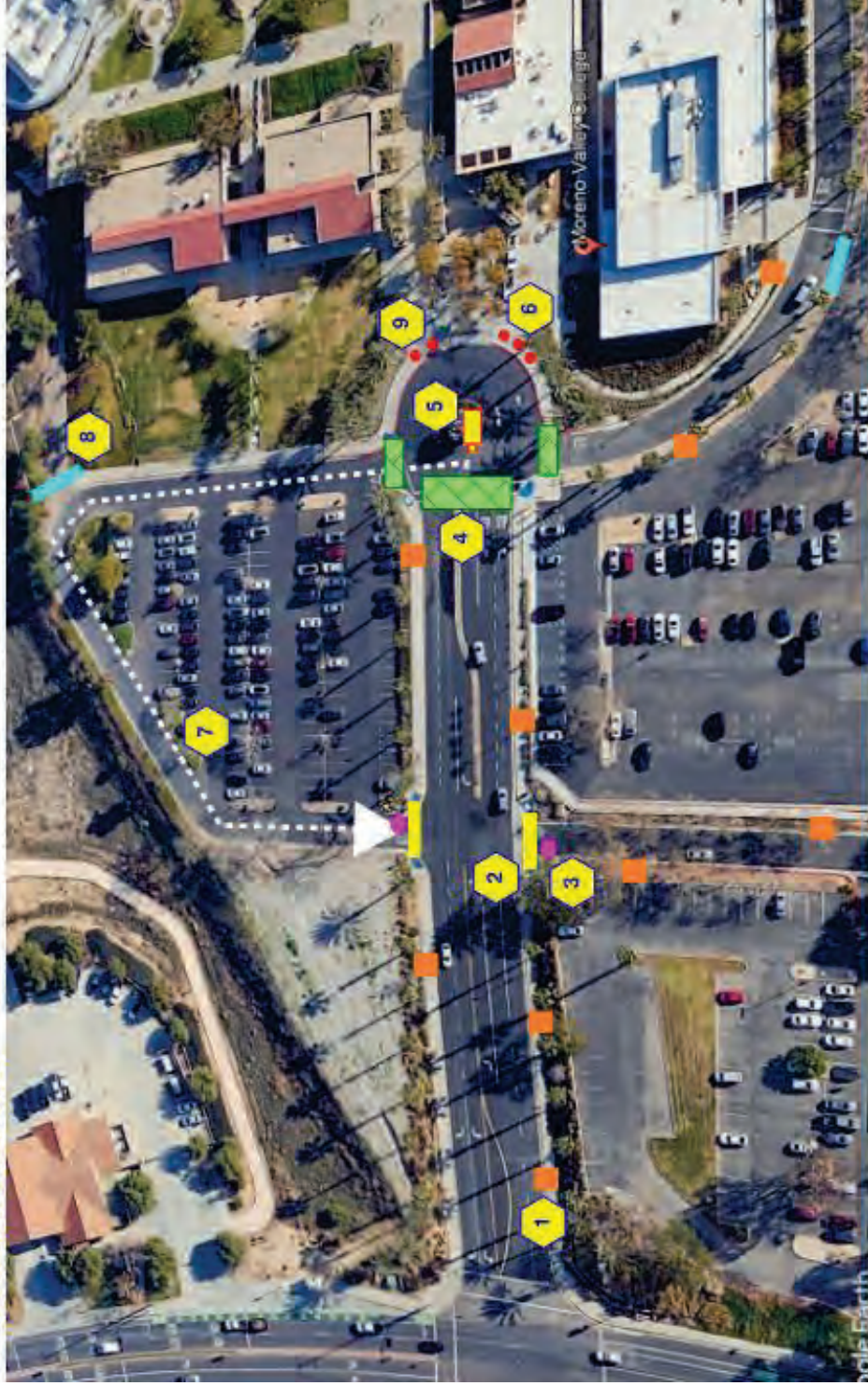
Landscape Vehicle Barrier - While bollards are obvious, effective anti-vehicle measures, there are many other engineered or rated solutions which can prevent vehicle impacts. The most effective and aesthetically appealing measures include raised planters which, through a combination of reinforced concrete, secure attachment to the ground, and the weight of soil and plants, provide substantial protection against high-speed vehicle impacts.

As with all safety and security measures, education of campus users is encouraged regarding the intent, purpose, and request to follow traffic calming measures. As well as education, enforcement of non-compliance is critical to strike the right tone that lack of conformity has consequence. Campus Police patrols in marked vehicles is also a means to traffic calming, with visibility deterring potentially bad behaviors.

The following mark-up snapshots provide illustration of potential speed calming measures that may benefit the MVC, College Drive and NC, Third Street traffic risks currently faced. Neither mark-up as illustrated in Snapshot 1 and Snapshot 2 respectively are intended to be finite solutions. They serve as suggestions for further evaluation with a subject matter traffic consultant expert. From a general safety and security perspective each traffic calming layout is intended to provide notification of approved speed limits, delineate specific traffic points of entry and egress, support speed reduction with rumble strips (deployed to support existing traffic light implementation), and identify means of existing and new measures to compartmentalize vehicular access.



1. SPEED CONTROL SIGNAGE
2. EXISTING SWING ARM GATES
3. RUMBLE STRIPS
4. RAISED PEDESTRIAN CROSSINGS
5. LICENSE PLATE RECOGNITION CAMERA
7. ONE-WAY TRAFFIC FLOW THROUGH THE PARKING LOT
8. FUTURE SWING ARM GATES (CONTROL BY ACCESS CONTROL AS NECESSARY)
9. REMOVABLE BOLLARDS



Snapshot 1: MVC College Drive Entry



1. SPEED HUMPS SIZED TO ALLOW UNRESTRICTED EMERGENCY VEHICLE ACCESS WITHOUT SPEED REDUCTION
2. RUMBLE STRIPS
3. LICENSE PLATE RECOGNITION CAMERA
4. RAISED PEDESTRIAN CROSSING
5. FUTURE SWING ARM GATES (CONTROL BY ACCESS CONTROL AS NECESSARY) ALLOWING ABILITY TO CLOSE ENTIRE CAMPUS TO PUBLIC VEHICLE ACCESS
6. SPEED CONTROL SIGNAGE
7. ONE-WAY TRAFFIC FLOW THROUGH THE PARKING LOT



Snapshot 2: NC Third Street

Fencing and Gates

Chain link fencing with slats provides the most cost-efficient means of fence installation with visibility restriction. It is recommended that regardless of fence material that minimum fence heights be 8' (10' preferred). Consideration should be given to limit the potential for bad actors to simply use the fence material to support their scaling of the fence. Some options are to use a 1" chain link providing some anti-climb deterrent or use 2" chain link with visibility slats. In addition to mitigating the climb possibility, these options will support restriction on the public or bad actors loitering and observing activity at sensitive areas i.e., ECEC at both MVC and RCC.



Figure 249 - Chain Link Fencing with Slats and 10' 2" Chain Link Fencing

An alternate to chain link is WireWorks Anti-Climb¹⁷ fencing that consists of welded wire mesh. This could be applied where restricting visibility is not a requirement. The anti-cut welded wire mesh makes it exceedingly difficult to get a foothold on this fence, and the cutting implements required to sever its welded heavy steel wire cannot fit into the minimal spaces of the mesh. WireWorks anti-climb is available in 10' height product, potential use of this fencing is suggested for areas such as the ECEC perimeter areas restricting ability for ease of scaling. This product should be used for specific purposes only with increase in cost in comparison to chain link. Additional benefit of the WireWorks anti-climb framework is that the framework can serve as a raceway for wiring, conduits and or security cabling reducing trenching and boring costs supporting ease of providing infrastructure to video surveillance, access control communications systems etc.

¹⁷ [WireWorks Anti-Climb | Ameristar \(ameristarperimeter.com\)](http://ameristarperimeter.com)

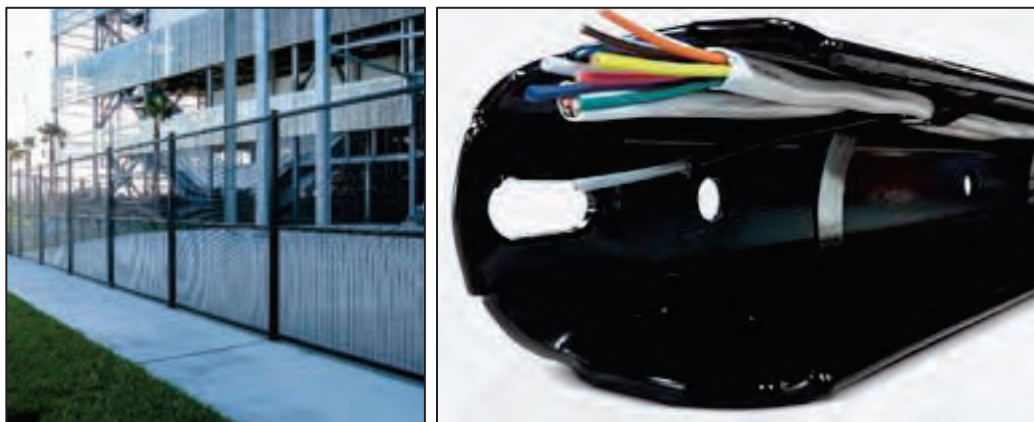


Figure 50 - WireWorks Anti-Climb Fencing and Cable Raceway

Decorative fencing has its place and provides several other benefits in addition to deterring bad actors and delineating secured space, including enhancing campus curb appeal and durability with minimal maintenance required. As identified within the findings, existing decorative fencing consists of flat top beams that encourage ease of scaling. Areas such as the swimming pool at RCC that are also shared space facilities with the public require consideration of fencing that is aesthetically pleasing to facility users. Although this is achieved, the security aspect of the existing fencing is marginalized by the low height and style of the fencing installed.

To improve security, we recommend using decorative fencing with spiked toppers facing straight up or outward. This will make it more difficult for intruders to easily climb over the fence. When choosing fence materials, it can be difficult to balance cost and security. Using design standards can help ensure that the right type of fence is chosen based on operational needs, security requirements, and budget allowance, providing a consistent look to district facilities.



Figure 51 - Ameristar Decorative Fencing

Signage and Wayfinding

Findings:

Signage is typically the clearest form of communication tool employed across community colleges with physical signage serving several different functions including wayfinding, safety, building identification, and accessibility. The approach taken to observation of signage and wayfinding was observing from a visitor perspective with the assessment team asking, “does the signage provide clarity of direction and information?,” and from a condition and content perspective, “is it legible and does it contain regulation reference to support enforcement of non-compliance?” A systematic process evaluated the layered security approach with observations starting at the site perimeter and working inwards, reviewing content and legibility with focus on analyzing if the message being communicated is consistent across the local campus, building, and district.

It is evident across the RCCD campuses and administrative buildings that there is no standardized governance in place relating to appearance (size, color, font size, text style), information displayed (i.e., inconsistent reference of video surveillance monitoring, information displayed, and signage placement). Buildings were identifiable by signage, with no consistency across individual sites to maintain a common feeling that all facilities are part of one college and a larger district.

Application of door numbering signage in general lacks a consistent application on the exterior of all openings to support potential first responder response to an incident. Roof signage identifying buildings by number or type is not applied at any campus or administrative building, visibility from above can be critical if air response is required for an emergency incident.



Figure 52 - Lack of Door/Opening Numbering displayed (RCC)

Many signs across the collective campuses need maintenance review with sun bleaching a common observation that has resulted in the intended information no longer being displayed or completely disappearing. Other maintenance related issues pertain to signposts being present but physical signage removed. Poorly maintained signage gives a negative impression that does not provide an immediate positive image for RCCD.



Figure 53 - Sun bleached signage at Third St. (NC)

Emergency call stations lack consistency of location identification supported by physical signage. Some call stations are identifiable with associated signage while others are not. Not all emergency call stations MVC have campus maps associated with them. Provision of campus maps at Call Stations is not a common practice across all campuses.

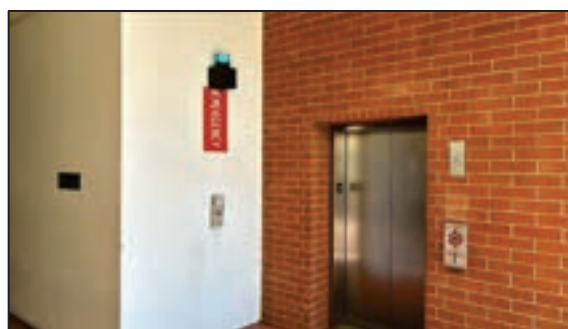


Figure 54 - Emergency Call Station signage (RCC)

General wayfinding maps are poorly distributed across all campuses, presenting challenges to visitors and other campus users unfamiliar with campus layout. It is difficult to identify current location and the desired travel endpoint. Campus maps in some cases (i.e., NC) have only one general campus wayfinding map on campus. The information displayed is dated and known to require updating. Placement of wayfinding maps lacks cohesion with no consideration to aligning map placement adjacent to parking lots pedestrian access points for ease of identification and observation. Digital, web-based, options are not made available to allow campus users to access maps via cell phones using QR codes.



Figure 55 - Wayfinding Signage at RCC and MVC

Emergency evacuation plans across all district facilities appear to be well deployed with focus on ensuring that they are displayed in all classrooms, an initiative that has been performed at all locations. The action taken regarding emergency evacuation plans display is excellent. There is, however, a lack of district driven expectation and direction regarding the imaging and material used to present the plans, resulting in local oversight rather than district management driving consistency in map appearance and material performance features. NC emergency evacuation maps are manufactured by Everlux and are compliant with NFPA 101 and NFPA 170. *NFPA 170, Standard for Fire Safety and Emergency Symbols, establishes the design principles of Evacuation Plans that are to be displayed throughout the building. These principles establish that the design of Evacuation Plans must include information relevant to fire safety, means of egress, and rescue of the occupants of the building. The Evacuation Plans shall be designed in accordance with the evacuation strategy of the building and address the specific needs of the occupants of the premises.*¹⁸



Figure 5625 - Emergency Evacuation Plans at RCC and MVC

The Everlux signs use photoluminescence to illuminate signs during periods of darkness and power outage. *Photoluminescence is the discharge of electromagnetic radiation (Photons) of a material after being submitted to a luminous excitation. The photoluminescent sign has the purpose of effectively transmitting the message for which it was manufactured, i.e., to show alarm equipment, fire equipment, safety equipment, etc. It also shows escape routes (exits, doors, etc.), the dangers, the obligations, or the prohibitions, guaranteeing total understanding, even in blackout situations.*

The Everlux plans in use at NC are market leading product and should be rolled out across all RCCD facilities as they provide visibility and sustainability benefits not associated with card maps observed at other locations.

Recommendations:

It is understood that at the time of writing that there is a standalone project regarding signage and wayfinding in process at NC. If this is localized it is recommended that the scope be expanded to encompass the other district college campuses, with focus on delivering a standardized and consistent feel to use of signage and wayfinding.

¹⁸ [Evacuation Plans and Fire Alarm / Sprinkler Zone Plans - Everlux](#)



It is recommended that a consistent appearance of signage across all campuses occur presenting a single RCCD image that will drive cohesion across the district sites and present a positive and welcoming environment for campus users. Currently MVC and NC have some alignment in appearance of signage and emergency plans in terms of color, a review and consideration of district standardization on appearance would be beneficial. Consistency of signage visually has wider implications than just physical appearance, it promotes community, belonging, identity, and efficiency in procurement.

Standardization of signage size, text, color, and font provides ability to communicate and display information in a clear and effective manner. Placement of signage will require individual campus operational consideration to determine maximum impact. Overload of signage placement and display is discouraged to prevent sensory overload occurring especially regarding speed control measures, resulting in communication intent being lost.

The district should consider implementing a regular review of signage from a governance perspective to ensure that information communicated is consistent with district policy and approved signage appearances. It is critical to the success of safety and security measures and risk owned by RCCD, that directions and their intent are well communicated, easily understood, and displayed at strategic locations. Well planned and managed signage installation removes the need for campus end-user assumption.

Priority areas for immediate review and consideration are improvements to wayfinding signage and application of door numbering at all doors to support first responder identification. Future consideration to building identification from above is also recommended for future consideration.

Wayfinding

Providing wayfinding signage provides clarity and direction for campus users and visitors and helps in maintaining pedestrian traffic order. People typically respond to direction, and the provision of clearly defined wayfinding signage is a cost-effective method of enhancing a safety and security program. If an expectation that visitors must sign-in on arrival at a facility (difficult to achieve in the community college arena) or make themselves known to persons visiting, providing direction to the sign-in location and specific buildings supports that. If visitors do not know where the sign-in location or building location of person(s) visiting is, this presents risk that they may wander into buildings unannounced causing potential disruption. Simple things can often have the greatest impact, and we recommend that the district evaluate its current wayfinding and consider an upgrade program to meet operational requirements.

Wayfinding placement should factor in areas of heavy pedestrian foot traffic, areas of congregation, access points from parking lots and bus stops into campus, maximizing visibility and ease of identification for use. Consider displaying less inconsequential text and emphasizing actual “You are here” position and other key safety and security information i.e., evacuation muster points and emergency call station locations. Wayfinding should not just be limited to physical signage; use of interactive dynamic mapping that can be accessed by mobile devices would provide significant benefits to simple static wayfinding maps.

An interactive digital mapping approach would provide some significant benefits over the traditional static physical signage approach. Firstly, the ability to immediately refresh and update maps with real-time information including most current directions and event schedules delivers a more engaging end-user experience. Digital mapping



applications offer significantly more benefits, including options to push and pull information as needed, and allows for enhanced features for people with disabilities with large text presentation and audio options. The visualization features that digital mapping offer are continually evolving with simple add-on imaging to locations of emergency phones, bus stops, parking lots, etc.

Typical features of interactive digital mapping include:

- Maneuverability
- Layered display of information, enhancing depth of purpose and intent
- Interactive video, imaging, and graphics, providing familiarity of surroundings.
- Visual Awareness
- Interface with 3rd party mapping providers, i.e., Google and Apple Maps
- Safety and security reinforcing of facility features, i.e., emergency phones, defibrillators, etc.

Digital mapping options using QR codes are becoming increasingly prominent within society and the education sector. The tendency for continual deference to cell phones for immediate information gathering makes the use of QR codes an ideal means of distributing information easily by simple scan of a code. Physical static wayfinding maps still have a purpose, but they can be supplemented by digital mapping that allow campus users to identify their position and intended destination location.

Additionally, the cell phone digital accessible wayfinding provides a platform for brand affirmation, distribution of interactive promotions, targeted messaging, as well as reducing paper waste with less static signage required.

The district has made efforts to digitalize mapping via the website, however links to maps are not currently available via QR code placement across campuses, and when accessed via the website, the maps are not always available, see Figure 57.

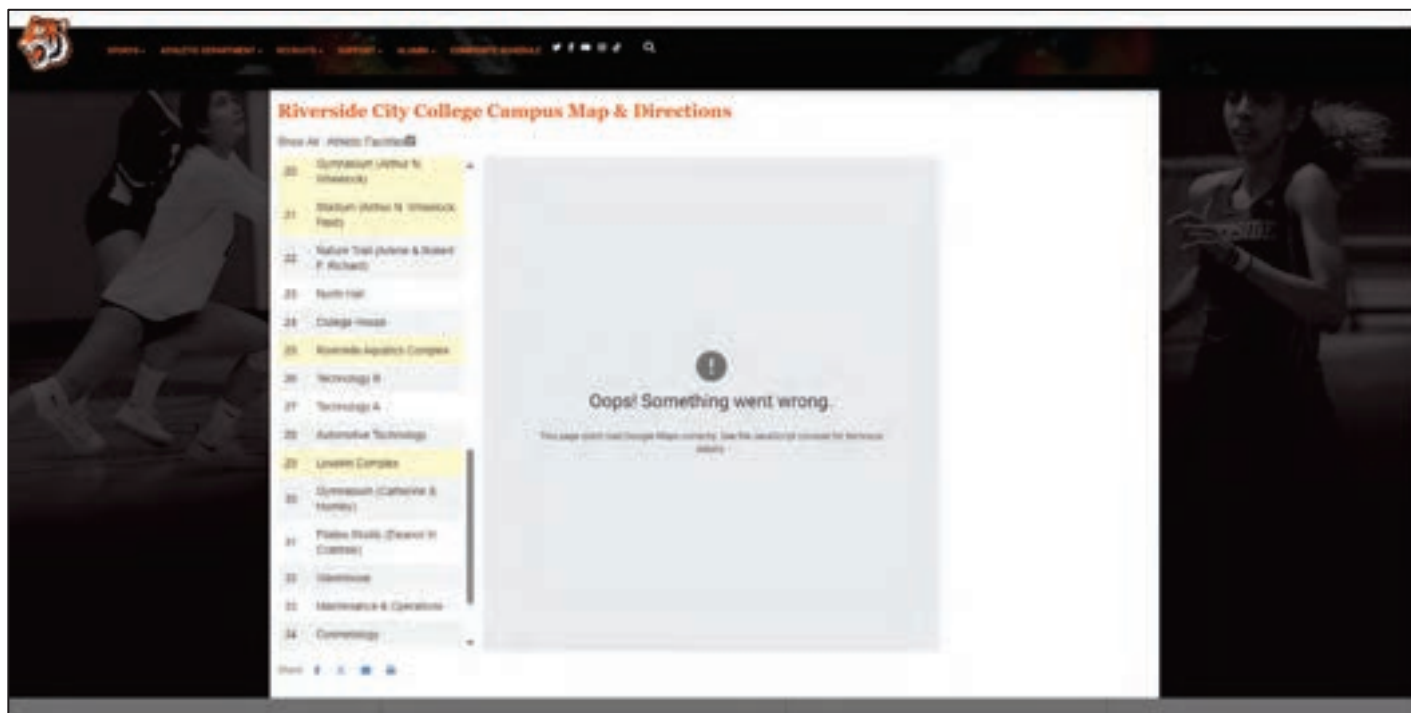


Figure 57 - RCC Digital Map

Door Numbering

Well-presented door numbering signage can provide first responders with critical extra seconds when responding to an incident if rooms are easily identifiable using clear and prominent signage. The simple application of room numbers to all interior and exterior openings provides a cost-effective means of enhanced incident location identification, supporting response efficiency. The use of door templates/stencils as illustrated in Figure 58 provides a simple solution to consistency of visual door numbering across all facilities. A critical component of door/room numbering application is that the physical room/door numbers are coordinated with any emergency building evacuation planning documentation. Strong ownership of the security program should proactively implement activity to confirm that door/room numbers match emergency building evacuation planning documentation. We recommend that the district implement a review and numbering upgrade plan to ensure that numbers are assigned correctly within evacuation plans and other emergency documentation.

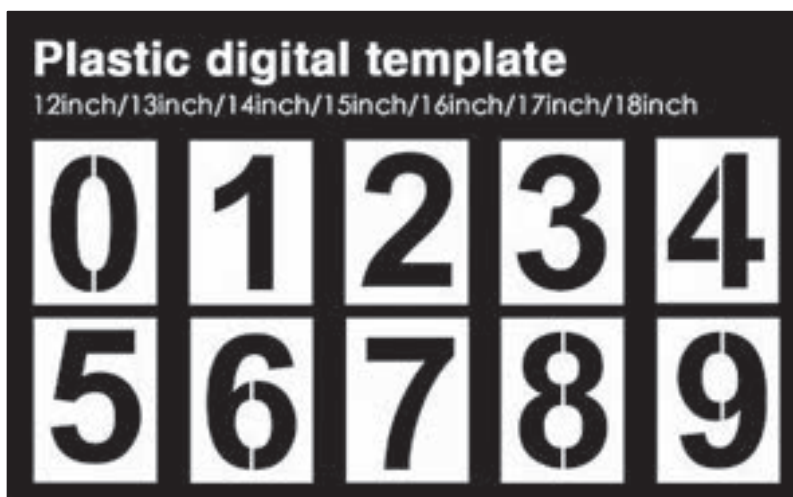


Figure 268 - Door Number Stencil

Building Identification from the Air

Rooftop building identification signage often goes unnoticed, yet it plays a crucial role in facilitating campus operations and emergency response. Clear and prominently displayed building labels offer a multitude of significant advantages:

- **Enhanced Emergency Response:** During critical situations such as fires, hazardous material spills, or natural disasters, easily identifiable buildings help emergency services to respond promptly and effectively.
- **Improved Campus Navigation:** Rooftop signage not only assists in aerial surveillance but also aids in providing clear orientation on the ground, particularly for campuses with expansive layouts or intricate designs.
- **Facilitated Maintenance and Repairs:** Clear building identification streamlines the coordination and scheduling of maintenance and repair services, contributing to the smooth functioning of campus infrastructure.
- **Enhanced Campus Security:** Clearly visible building labels serve as a deterrent to criminal activities by complicating intruders' ability to navigate the campus discreetly.
- **Improved Campus Aesthetics:** Thoughtfully designed rooftop signage can enhance the overall visual appeal of the campus, contributing to a more pleasing and welcoming environment.

Immediate investment in rooftop signage is not required as the prior wayfinding and door/room identification measures are more pressing. Rooftop signage should be a future consideration and documented within future security program design standards. Minimum baseline expectations should be documented serving as reference that all design and construction projects apply appropriate signage measures accurately and consistently. Rooftop signage can enhance safety, operational efficiency, and overall campus experience.



SECURITY ELECTRONICS TECHNOLOGY

Access Control

Findings:

The current RCCD access control system is manufactured by Software House, a Johnson Controls company. The platform is CCure 9000, a powerful and flexible security management system that supports full integration with video surveillance and intrusion detection. The district in its current use of the CCure 9000 access control system does not interface any access control or intrusion detection alarm events i.e., door forced, or door held alarms with video surveillance camera call-up. Varying versions of the CCure 9000 systems software are in use across the district campuses with no centralized management of software support agreements, service level contractor agreements in place, and no centralized management and oversight of the system from a district position. The current (at time of the assessment) software versions and software support agreements (SSAs) types in place at each campus are illustrated in Table 11.

Campus	Serial #	Version	SSA Type	Expiration Date	Server license
RCCD	9-13657	2.8	Enhanced	6/30/25	R+
Norco	9-10663	2.9	Enhanced	3/31/24	R+
Moreno	9-12194	2.9	Standard	5/31/27	Q

Table 11 - Riverside Community College District CCure Licensing Information July 2024

The different software versions and SSA types currently active provide a lack of consistency in systems performance capability and the level of support response that is received from Software House. For example, the software version 2.8 in use at RCC is technically no longer supported by Software House who service version 2.9 or above. The SSA level at RCC which is “Standard” provides support through business days 9:00 AM to 5:00 PM only, in contrast MVC and NC have 24/7 support with the “Enhanced” service agreement level.

All existing CCure 9000 deployments are standalone systems failing to capitalize on the enterprise level topology typically found with large deployment of access control as observed at RCCD. The administration of each campus system occurs locally, with no dedicated primary function resources for management and administration. The local systems administrator activity varies across each campus from general issuance of security credentials to activation of lockdown of electronic hardware. Staff training on systems varies from self-taught to participation in manufacturer training events (noted that the training was not the appropriate level for a systems administrator and was more targeted at systems installers). Furthermore, existing systems administrators must be located at their workstations to access the system, including when activating a lockdown as no utilization of access via mobile application is in use.

Existing CCure 9000 Software House hardware for the majority of installations is deployed using legacy proprietary iSTAR Pro and iSTAR Ultra SE intelligent controllers wall mounted in enclosures or rack mounted in network equipment racks. Power supplies are typically manufactured by Altronix providing power outputs to electrified door

hardware. Application of typical components associated with access control doors including card reader, request-to-exit switch or motion sensor, door position contact, electrified hardware, and mechanical door closer were not installed consistently at every controlled opening. Several interior controlled openings were equipped with card reader and electrified hardware with no ability to monitor door position status. Inability to monitor door position status effectively means that the access control system is acting as an expensive brass key only, as no audit trail is created of who accessed an opening and when, or if a door was forced or left open. An observation of note is that at many critical infrastructure network rooms, controlled permissions-based entry requires presentation of a security credential with authorization to enter. This same level of security is not applied to the District Office Room BDF 205 which is accessible by brass key only, access could not be gained into this space by the assessment team (it is assumed that systems servers are housed within).

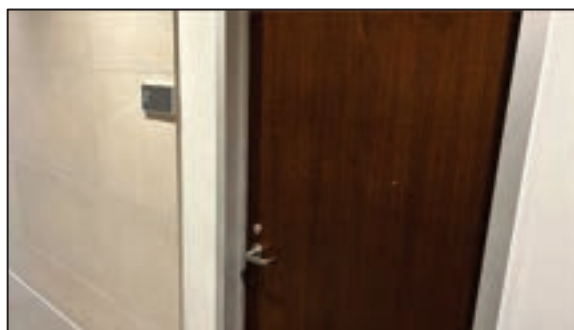


Figure 59 - District Office Room BDF 205

Card Readers

Several different types of card readers are in operation throughout the district campuses and buildings with Software House RM card readers commonly observed. The RM readers house embedded HID multiCLASS card readers supporting several enhanced security encryption communications used by smart card credentials. The readers also have 12-button keypads that can be used for entering Personal Identification Numbers (PINs) to arm and disarm intrusion monitoring. NC currently has the access control system programmed to immediately place either specific buildings related to a specific keypad location to enter lockdown mode (locking of all electrified openings) or have the electrified hardware for all buildings across campus to be placed into a locked state. Input of unique local PINs per building and a separate PIN for campus lockdown input at any card reader activates the appropriate action. RM readers support toggle locking and unlocking by presentation of an authorized security credential with quick taps. This is convenient for faculty to keep classroom doors unlocked during crossover periods.



Figure 60 - Software House RM Card Reader Keypad and Siemens (HID) RP40 Card Reader

Other card readers observed were HID multiCLASS SE RP40 devices. The multiCLASS SE RP40 is part of HID Global's iCLASS SE platform for adaptable, interoperable access control. Designed for multi-factor authentication door applications requiring standard wall switch mounting, multiCLASS SE RP40 supports a broad array of 13.56 MHz high frequency and 125 kHz low frequency credential technologies and a variety of form factors, including cards, fobs, and mobile devices.

Security Credentials

Access credentials in use across all locations vary in appearance but appear to be HID iCLASS cards. Security credential appearances differ across campuses with photo images applied at RCC and NC, but not at MVC. Security credentials function as informal identification badges when photo images of the authorized credential holder are applied. There is no district policy in place that governs appearance or display of either security credentials or identification badges in general. The iCLASS credentials use the 13.56 MHz frequency rather than the 125 kHz frequency, this is excellent and reduces the ease of potential credentials being copied (the assessment team was unable to copy a District access control card with an off the shelf copying machine).



Figure 61 - HID iCLASS Credentials



Lockdown and Duress Buttons

Lockdown and duress buttons are used across several campuses and district facilities with no standardized approach to their application. Each campus has its own approach to applying lockdown and duress buttons. The predominant communication method of the devices is through wireless, rather than hardwired, communication. Mobile buttons were observed including at the District Office Cahiers Office, this could potentially result in a button being intentionally or unintentionally removed, resulting in the inability to be located, and used if needed. RCC is currently rolling out a campus-wide electronic lockdown deployment at locations where Software House RM card readers are not currently installed. The wireless buttons provide flexibility of installation. However, during the assessment observations were made of buttons being installed at wall locations on the outside of secured departmental spaces, providing potential tampering opportunity. Signage was also lacking identifying the intent of the buttons as well as stating consequences of misuse. Buttons have no covers and there is no approach for installing video surveillance at each lockdown button location to provide immediate camera call-up or forensic review when a button is activated. Wireless lockdown buttons in addition to flexibility of placement, provide a cost-effective approach to installation with no requirement for cable pull and termination and increase availability to activate lockdown from areas that may have challenges with hardwired installation. Challenges posed by wireless devices that must be considered by the district include battery status monitoring which is critical to ensure power is provided when activated, communication verification with the system head-end ensuring as best possible immediate uninterrupted communication with no latency, frequent and documented testing with immediate corrective action if faults or issues identified, and firm affixing of buttons to desk undersides or walls to eliminate ease of removal. Activation of lockdown across all campuses remotely is currently not an option as not all buildings are equipped with electronic hardware. Existing lockdown requires a mix of mechanical securing of doors and remote locking through the access control system.

Duress buttons observed were predominantly DMP dual button devices that require two independent buttons to be depressed for two seconds to initiate an alarm. Other duress buttons observed included momentary activation buttons. Application of duress buttons is not consistent. For example, at the RCC Financial Aid transaction counter they are not installed at each workstation. This also occurs at the Center of Social Justice and Civil Liberties front desk. This deployment style requires employees requesting assistance to physically leave their workstation to activate a duress button causing delay of immediate notification and potentially causing additional risk and exposure to themselves as they must turn their backs to leave their workstations. It is understood that the duress buttons communicate out through the access control system to the intrusion detection system monitoring station. The offsite monitoring station then alerts the Riverside Sheriffs Dispatch who then notify campus police for response.

Of concern during the assessment was the lack of knowledge and awareness of the provision of duress buttons by employees. Several interactions with staff including at the District Office HR Department front desk clarify that awareness of availability of a duress button installed under the desk is lacking. Provision of both lockdown and duress buttons should be supported by comprehensive guideline and training material, and physical practice of use at least annually.

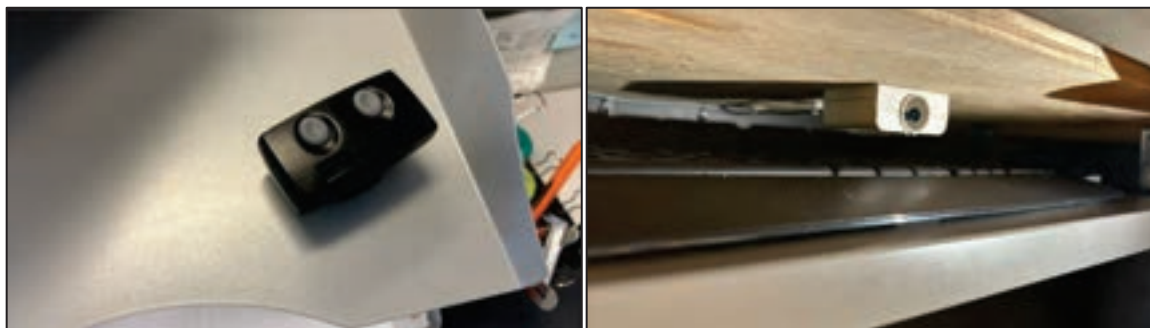


Figure 62 - Wireless Mobile Lockdown Button at District Office Cashiers Office and Momentary Pushbutton at Financial Aid Office at RCC



Figure 63 - Wireless Lockdown Button RCC

Intrusion Detection Interface

The CCure 9000 access control system supports integration with the existing DMP (Digital Monitoring Products) intrusion detection system. This integration allows system users to manage both systems through a single interface, enhancing operational efficiency and security. It is not confirmed that the district currently use the single interface management option that is available. It is confirmed that the two systems are integrated for provision of lockdown and duress button activation communication.

Norco Innovation Center

The Norco Innovation Center access control system is (per district employees located at the site) not owned or managed by the district. The building is occupied by a tenant who was the former owner of the building, they are understood to still have administration rights to the access control and video surveillance systems. The systems are Honeywell and the on-site district employees have web portal access only that allows them to add permissions to security credentials only. In addition to the lack of ownership of the security systems the security credentials in use are HID Prox Card II which are legacy technology and less secure than the credentials used across other facilities. Tenants should not have access rights to the district owned building security systems. Tenant space only system access should be permitted with the tenant providing their own independent security systems. The systems administrator does not monitor alarm events on-site. Implementation of a CCure 9000 or alternate district standard owned system should be installed.



Summary

In summary the existing CCure 9000 access control systems on each campus, although robust and able to serve the district from an enterprise level, have a lack of central systems ownership, local dedicated systems administration resources, monitoring and response to alarm events, gaps in application of electrified hardware, and lack of standards that minimizes the system's ability to serve as a "force-multiplier" to security staffing and district police. This should not be seen as a poor reflection on the system.

Head-end equipment is nearing end-of-life, is no longer supported by the system manufacturer, and disparate SSA's and SLAs provide no common end-user experience expectations. The system is operable to provide the district with its basic needs, and it can integrate with video surveillance systems in addition to the existing minimal DMP intrusion detection interface.

The ownership, system topology, operational intent of use, and training, are all key areas along with lack of standardization of application across the district, which should be reviewed and corrected as part of future access control utilization considerations.

Recommendations:

Fundamental to future maximization of investment and realization of benefit that access control can bring to the District is the need to identify a District systems owner, with localized dedicated support resources who can administer and monitor the systems as primary functions across all campuses and buildings. Application of access control measures in a standardized manner with allowance for individual nuance conditions to be addressed on a case-by-case basis is recommended. The standard approach should not only apply to location of device installation but also the components i.e., card reader, door position monitoring contact, request-to-exit switch/motion sensor, electrified hardware, and installation of mechanical door closers to support positive latching upon exit. Formalization of a standardized application of access control measures as with any standards provided governance and baseline minimum expectations.

Existing System Consideration – Migration Plan

The existing Software House CCure 9000 access control system is a solid enterprise system and will provide RCCD with a reliable foundation for future upgrade and expansion of access control measures, with interface to other systems. The CCure 9000 enterprise access control system can provide the district with a fully unified platform across all of its facilities with ability to centralize management and reduce physical metal box on-premises hardware. This system should, by design, integrate with building intrusion alarm and video surveillance systems to provide technology capability to serve as a "force-multiplier" to existing security staffing and district police measures.

Considerations of a potential upgrade path for the Software House CCure 9000 solution include:

- Upgrade existing iSTAR Pro and iSTAR Ultra SE intelligent controllers to iSTAR Ultra G2 controllers that support up to 32 card readers per controller. Additional features of the Ultra G2 controllers:
 - Powerful cyber-hardened network door controller



- Hardened Linux embedded OS for improved security and scalability
- Power over Ethernet (PoE) module features PoE+ to power the (GCM) General Controller Module
- Up to 1M cardholders in local memory
- Embedded lock power management lowers installation costs
- Advanced controller-to-controller communications for cluster-based anti-pass back and I/O logic
- Onboard 256-bit AES network encryption
- Supports OSDP Secure Channel for encrypted reader communications.
- Retrofitting iSTAR Ultra G2s into existing enclosures would provide bulk buy pricing incentive, the same could be applied to procuring new LifeSafety Power Supply enclosures for door lock power.
- Upgrade the existing CCure 9000 software to at minimum version 3.0 or target version 3.1 that is scheduled for release in 2025.
- Consider transitioning to CCure IQ that provides the ability to manage and monitor both access control and video surveillance using an internet browser from any PC or tablet, removing existing minimal local workstation sign-on access providing greater flexibility for immediate viewing of activity when required.
 - Key features of CCure IQ includes:
 - Personnel Management: Easily manage personnel records, assign clearances, and monitor video tours.
 - Alarm Monitoring: Adaptive event viewing options for proactive response to critical security risks.
 - Video Surveillance: Native video surveillance for live monitoring and forensic search.
 - Security Intelligence: Prioritizes vital alarms, improving operational efficiency.
 - Customizable Layouts: Choose pre-configured or create custom layouts tailored to your security team's roles and responsibilities.
 - Optimized for VideoEdge NVRs: Enhances live monitoring, smart streaming, and forensic search workflows.

One challenge of a system hardware upgrade can be the availability of physical space for panel enclosures and power supplies in equipment closets. Reduction of space requirements could be achieved by transitioning from Altronix standalone 12 and 24 VDC power supplies to LifeSafety Power enclosures that combine intelligent access control system controllers and other boards along with system power, lock power and distribution. These panels can be pre-wired at the factory supporting efficiency of installation and reduce in-demand and restricted real estate space for mounting. LifeSafety Power prewired enclosures are available for several other leading access control systems and not just for Software House. Consideration of LifeSafety Power use for alternate systems solutions is recommended with the same space saving consideration as the driving reason.

Alternate Systems Evaluation

As security electronics continues to evolve and technology provides support to other physical security measures, the current age and lack of systems integration of RCCDs existing campus access control systems provides an opportunity to evaluate alternate solutions before finalizing any decision on a future direction to take. When it comes to evaluating and selecting systems, the process can be complex. It is recommended that the District consider up to three (3) enterprise level solutions in addition to a review of the existing systems providing insight, observation, and

perspective of alternate solutions that may enhance RCCDs security operations. Systems selection evaluation activity typically involves reviewing at minimum:

- Systems identification, on-premises, cloud, hybrid dependent upon district would-likes.
- Demonstration coordination, plan ahead with key “would-likes” provided to the systems manufacturers to support a defined and focused demonstration.
- Systems technical performance evaluation baseline, evaluate on an “apples-for-apples” basis.
- Use of feedback templates for stakeholders ensuring a cross section of key users are invited to demonstrations and provided the opportunity to give feedback.
- Infrastructure topology identification
- Identification of certified local systems vendors and installers, important to understand who is available to provide local support and their levels of certification.
- Evaluate systems and make informed decisions based on key factors listed above.

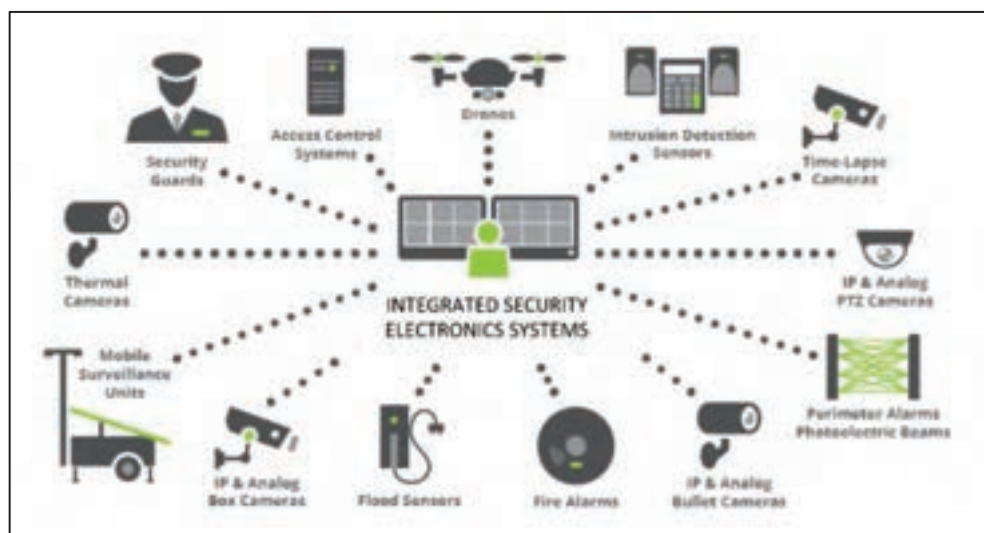


Figure 64 - Integrated Security Electronics Systems

The thorough review of system features and performance parameters is central to ensure that operational needs can be provided by selected solutions during the system evaluation process. It is imperative to assess the capacity of the system’s ability to operate within an enterprise environment and enhance the effectiveness of the RCCD security program. Collaboration during the systems review phase amongst district key stakeholder groups is needed to facilitate the definition of RCCD’s specific requirements for unique system feature sets such as alarm event notifications, camera call-up, automated incident notifications, and local and remote lockdown capabilities.

Alternate access control solutions for consideration that offer a variety of on-premises, cloud, and or hybrid operating system include:

- Avigilon
- Lenel S2
- Honeywell



- Vanderbilt
- Verkada
- Genetec
- Panasonic
- Open Options

Standardization of Equipment

It is recommended that the district standardize on access control equipment supporting interoperability of components within the wider enterprise security solution that is decided upon as the district platform to move forward with. A formal Division 28 Electronics Safety and Security standard should provide approved product lines and date sheets for reference. Standardizing on the equipment will provide cost efficiencies in equipment procurement and provide a consistent appearance and functionality of security devices across RCCD campuses and other facilities. The standardization approach will also maintain minimum-required levels of security across all facilities regardless of budget.

Hardwired Lockdown and Duress Buttons

Built environment conditions and cable pathway restrictions can present challenges in providing cable to lockdown and panic buttons for direct termination to the access control and intrusion detection system control panels. However, where possible it is encouraged that hardwiring of such devices be the standard practice with flexibility permitted for areas where it is deemed not possible due to lack of pathway, or the cost factor is prohibitive. Hardwiring of emergency notification buttons supports mitigation of the potential issues noted previously related to wireless communication buttons. Hardwiring allows for supervision of power, reduced likelihood of loss of communication, secure and permanent installation, and efficient integration through inputs and outputs with other system components (i.e., strobes, horns, cameras etc.).

Security Credentials – Photo Identification

As observed, the existing iCLASS credentials appear to use the encrypted 13.56 MHz frequency rather than the easily copied 125 kHz communication frequency. The card type and appearance should be standardized across RCCD along with policy regarding their display. The sample security credential badge shown in Figure 65 illustrates an existing MVC security credential where the credential owner had personally added a photographic image of themselves to the badge. It is recommended that the practice of photographic images of the authorized credential holder be applied as typical across all RCCD security credentials. Use of photographic identification can enhance the security program in a variety of ways. Visual verification discourages imposters from using someone else's credential when a culture of challenging things that do not appear right is established. Photo identification supports verification of persons via the video surveillance system if their image is stored, and also supports verification of persons making unauthorized entry attempts at controlled openings where they have no permission to enter. Persons displaying credentials support positive reinforcement that they are authorized to be in secured spaces and help employees and visitors identify each other. Policy is required to govern both the security credential information displayed and the use and display of credentials. It is important to factor that photo images cannot be displayed on other types of security credentials such as fobs or can be "hidden" if mobile credentialing is used. Security cards should be considered for issuance as the

standard district means of identification for all staff and employees, rather than issued when a person requires access to a space that is access controlled, as is the current process. Other credentials such as mobile credentials may be used but they should not be the primary credential issued across District facilities.



Figure 275 - MVC Security Credential

Intrusion Detection

Findings:

Several different intrusion detection systems were observed in use across district campuses and facilities. Intrusion detection components typically included door position monitoring contacts and motion detectors. Arming stations varied from standalone keypad to keypad and separate card reader, and keypad card reader combination units. Locations with card readers provide the district ability to review who and when a system was armed or disarmed via an audit report, typically the intrusion detection systems are armed and disarmed by day and night custodians with buildings monitored for a short period of time as often night custodians work until early morning. Monitoring of systems is contracted by off-site, third-party monitoring companies with a communication tree that provides notification to the Riverside County Sheriff's Dispatch Office who then notify district police when an alarm is received.

Some locations (i.e., RCC) where access control is installed at openings also monitor those openings on the intrusion system. Hardwired termination to both systems is in place. This is excellent and maximizes one door position monitoring contact to serve both systems. Intrusion detection systems are in widespread use, but they are not deployed at all district buildings as a standard. Inconsistency in distribution of codes and credentials for arming and disarming of the systems is also evident. Some systems require input of a "unique" individual 4-digit code and others use card reader as stated. Use of codes provides risk as they are often shared amongst others providing immediate vulnerability to the security of a building if disarmed by a person without authority to do so. Individual building and campus-wide codes are input at the Software House combination RM card readers to activate local and campus wide lockdowns.

The predominant intrusion detection system in use is the DMP system that interfaces with the CCure 9000 access control platform. This integration allows users to manage both systems through a single interface, enhancing operational efficiency and security.

Some key features and benefits of the DMP CCure 9000 interface:

- Unified Management: Users can monitor and control intrusion detection and access control systems from a single platform.
- Event Synchronization: Intrusion events can trigger access control responses and vice versa, improving situational awareness and response times.
- Scalability: The system can support a wide range of configurations, from small standalone setups to large enterprise environments.
- Enhanced Security: Integration helps in creating a more comprehensive security solution by combining the strengths of both systems.

At several locations, the interface between the systems simply consists of a CMP communicator providing alarm events received within the CCure 9000 platform to be communicated out to the off-site monitoring company. Several Bosch arming stations were also observed across some buildings, the Bosch systems are understood to be non-operational.



Figure 66 - MVC Intrusion Arming Station w/ Card Reader and Software House RM Card Reader



Figure 67 - Bosch Arming Station

Recommendations:

The District's current operations would benefit as with other security electronics systems from a standardized approach to intrusion detection application. The use of intrusion detection components is currently well deployed but inconsistent. It is recommended that the district use a single brand of intrusion detection system that interfaces



with access control (i.e., DMP) and further develop the integration with existing access control and video surveillance systems. Ensuring that an open-source system is used is typically critical to future scalability and interface with other systems to allow technology to serve as a force multiplier to Police, security staffing and operations. Fundamental to future intrusion and other security systems deployment and realization of value are the following:

- Develop security standards that become a reference point for future new construction or security upgrade projects that will serve as a reference point and support consistent deployment of security technology including the intrusion detection components.
- Install door position monitoring contacts at all perimeter openings to provide an envelope layer of security at each building perimeter.
- Integrate the intrusion detection system with access control and video surveillance to create a unified platform, this would further:
 - Maximize investment made.
 - Supports integration of alarm events with video surveillance
 - Enhances response to door forced and door held alarms.
 - Takes advantage of existing systems in place
 - Provides audit trail of arming/disarming times and by whom (already available at card reader arming station locations)
 - Controls access into the facility to approved persons only after hours.

Intrusion detection systems use multiple different components to provide notification of a breach of security. Depending upon the application, the following devices are typically associated with an intrusion system and should be considered by the district at the development of standards (some are already used, but inconsistently):

- **Door Position Contact** – these are static devices (reed switches) that use a magnet to generate notification when the magnet is moved away from the contact. Door position switches are the most common form of intrusion device. Use of Double Pole Double Throw (DPDT) contacts provides dual monitoring capability for both intrusion and access control systems.
- **Motion Detection** – motion detection generates an alarm event when there is a change within the static space that the motion detector is protecting. Motion detectors are available in multiple performance types including long-range detection (ideal for corridors) and radial 360 detection (ideal for classrooms and office space). These detectors provide protection for different applications and should be selected accordingly. Infrared detectors are typical within the education market, and they can be either active detectors or passive infrared detectors.
- **Vape Sensors** – now commonly being used by education institutions to detect vaping, these sensors identify change in air quality using an air quality index (AQI) and provide an alert when a change in set parameters occurs.
- **Glass Break Sensors** – these detect impacts that causes glass to break. The sensors detect a pressure change occurring at point of impact on glass and glass that shatters on the ground.
- **Duress and Panic Buttons** – duress and panic buttons wired to the intrusion panel provide an immediate



notification to the offsite monitoring station and, if programmed and integrated with other systems, provide immediate local notification of the activation, and need for response. Policy and procedure are critical to ensure that activation is responded to efficiently and correctly.

All devices and control panels, including arming stations, are recommended to be installed at locations using a consistent approach. Use of a security device placement matrix would help identify to systems designers the typical locations that intrusion detection devices must be installed. The exterior shell of all campus buildings should be equipped with a protective barrier that supports identification of any breach into the building. Monitoring and planned response are vital to an intrusion detection system application and performance.

As with all systems, following installation, it is recommended that the district implement regular testing of all system components. The district should not assume and rely upon vendor test reports as acceptance that all systems function as intended. Regular planned maintenance and testing should be scheduled and recorded. The auditing of information should become a standard process. It is also recommended that service agreements be entered into with vendors who are manufacturer-approved and certified to perform maintenance work on equipment.

It is recommended that the district transition all non-DMP systems to the DMP intrusion detection alarm panels as a standardized solution providing ability to interface with other security electronics systems. Transition to cellular communication where not done would also modernize the system and reduce the requirement for provision of plain old telephone (POTs) lines, reducing infrastructure costs, potential points of failure, and enhancing communication capability to the monitoring vendor. Additional network connection and systems integration would allow for management and administration of the intrusion systems locally by an assigned security systems administrator.

Video Surveillance

Findings:

Video surveillance deployment across the RCCD facilities is varied by campus-to-campus and building-to-building. The district lack any cohesiveness in the existing systems and edge devices deployed, with no governance in place or system ownership that provides direction on video monitoring and use. Interviews with key stakeholders identified that video surveillance system deployment is typically left to the discretion of design and construction teams, with IT involvement limited to provision of network connectivity for edge devices and network video recorders. Centralized management of the systems and storage is not a current practice and typically network video recorders are installed on a building-by-building basis which is inefficient from a management perspective. Systems management after installation of video surveillance, lacks accountability to ensure that systems software agreements are maintained, and software updates received. Several different video surveillance systems and edge device manufacturers were observed in use across district facilities including:

- American Dynamics
- Sony
- Honeywell
- Axis



- Pelco
- Verkada
- Bosch
- Panasonic
- Tyco

Existing System

The most common video surveillance system in use is the American Dynamics Victor¹⁹ platform that when used as a fully integrated enterprise solution allows command and control to seamlessly synchronize video surveillance with access control, fire, intrusion, and other systems into one powerful, intuitive interface allowing the district to manage their operations more safely and intelligently. The systems capability currently is untouched by the district to support operations partly due to the lack of trained dedicated systems administration resources. Significantly due to a lack of district security program oversight, and security program ownership identifying how security technology can be better used to maintain safe and secure environments. Further dialogue with Software House and American Dynamics identified that several systems licenses had expired resulting in new software patches and upgrades not being received and potential new feature sets not made available. Table 8 illustrates in red expired licenses and varying versions of software in use. It should be noted that older American Dynamics network video recorders (NVRs) may not support the current software version of 6.0 rendering the NVRs near end-of-life.

American Dynamics Licenses and SSA's							Software House		
Serial Number	Current Expiry	SSA Type	Version	Model	Model Description	Last Recommended Version	E. Company Name	E. ADDR	E. City
NV90802223478	6/30/2021	Standard	5.9	ADV808000			MVC	5141 Galena Ave	Riverside
NV9081120100004	6/30/2020	Standard	5.1	ADV82490000			Norco College	2001 1st St.	Norco
NV5120120120194	6/30/2020	Standard	5.6	ADV81200A20			Norco Veterans Ctr	2001 1st Street	Norco
NV4081701120047	1/31/2024	Standard	4.2	ADV80290000	RTB	5.2.2	Norco College	1st Street	Norco
ES110310154754	2/28/2027	Standard	4.0	ADVCC000			RECD	2355 Wayne	
NV3100405175933	2/28/2023	Standard	5.0	ADV80490000			RECD	2355 Wayne	
E3699320110000	10/11/2022	Standard	5.6	ADV45000			RECD-MVC College	301 Market Street	Riverside
ES1111300000004	1/26/2021	Standard	5.1	ADV62000			RECD	301 Market Street	Riverside
NV9022201000000	1/31/2021	Standard	3.3	ADV800000000			RCC	301 Market St	Riverside
NV404150151000	2/28/2021	Standard	4.6	ADV80000000	RTB	5.4.1	Riverside Community College District	301 Market Street	Riverside
NV412040151000	2/28/2027	Standard	3.7	ADV81200A20	2U IPB	6.0	Facilities Planning and Development	301 Market Street	Riverside
NV412170152700	2/28/2027	Standard	5.7	ADV81200A20	2U IPB	6.0	Facilities Planning and Development	301 Market Street	Riverside
NV412170151500	2/28/2027	Standard	5.7	ADV81200A20	2U IPB	6.0	Facilities Planning and Development	301 Market Street	Riverside
NV3100002010000	6/30/2021	Standard	3.7	ADV810000000			Facilities Planning and Development	301 Market Street	Riverside
NV3100001010000	5/31/2025	Standard	4.1	ADV80000000			Riverside Community College District	301 Market Street	Riverside
E30009420110000	1/26/2023	Standard	4.9	ADVCC000	Video Express	5.3	Riverside Community College	400 Magnolia Ave	Riverside
NV400070170700	1/26/2021	Standard	4.9	ADV80000000	2U IPC	6.0	Riverside Community College	400 Magnolia Ave	Riverside
NV400020150400	1/26/2021	Standard	4.8.1	ADV81000000	2U Hybrid B	6.0	Riverside Community College	400 Magnolia Ave	Riverside
NV412040151000	1/26/2021	Standard	4.8	ADV81200A20	2U IPB	6.0	Riverside Community College	400 Magnolia Ave	Riverside
E3601501150400	1/26/2021	Standard	4.1	ADV60000			Riverside Community College District	400 Magnolia Ave.	Riverside

Table 12 - Riverside Community College District – Video Surveillance – America Dynamics Licenses and SSA Status

¹⁹ [59051 \(americandynamics.net\)](http://59051.americandynamics.net)

Network Video Recorders

Differing, NVRs offer different video retention, framerate, and resolution rates with no district standard available as governance. Lack of governance associated with video retention and access rights is concerning as it is important to ensure compliance with its own district policy (when developed) that video footage is retained, identify who can access it, and under what circumstances. A well-defined policy ensures that the district complies with its own governance, and it helps to avoid penalties, fines, or legal disputes related to mishandling of video data. For example, signage at the STEM Center at NC indicates that video surveillance is monitoring all activities that are recorded to aid in the prosecution of any crime committed against the facility. This could be problematic if the district is subpoenaed to provide video footage as the cameras are non-operational. Furthermore, signage does not indicate the duration of video storage retention. The District should establish a video retention policy noting the duration for which recorded video will be kept mitigating risk in the event of a request to retrieve recorded video.



Figure 68 - American Dynamics NVR



Figure 289 - Panasonic NVR

Management and location of NVRs lack best governance with several NVRs observed outside of areas where they are typically housed as best practice within secure data closets/rooms. For example, Figure 66, above illustrates a video storage unit located on the top of a wall mounted cabinet at the Cafeteria at MVC. Lack of secure housing of storage units can provide wider vulnerability implications including risk of cyber-attack if bad actors are able to access live network ports that support the video retention equipment easily. The different installations of NVRs across the district also fails to support any standardized or consistent approach to cable management and cable labeling. Lack of

installation standards and best practices adds challenges to potential service and maintenance activity as time is spent having to sift through unmarked cables to identify the point of issue. Climate control of data rooms is not consistent. Some rooms were excellent in application of HVAC units, drip trays or plumbing and temperature sensors, others had none.

Camera Types

Camera types in use in the district vary. As previously listed several different camera manufacturers' products were observed including cameras that are no longer available in the marketplace (Sony) and cameras that lacked power and were non-operational (see individual site findings). A common theme across the college campuses was the assumption that many cameras are non-operational. Cameras that are non-functioning is problematic as their intent and purpose to provide visibility of activity is not achieved leaving gaps and vulnerability in the security program compromising safety. Of equal concern is the accepted commonplace understanding amongst many campus staff and employees that cameras do not work, this fails to develop confidence in the security technology deployed.



Figure 70 - PTZ Exterior Camera

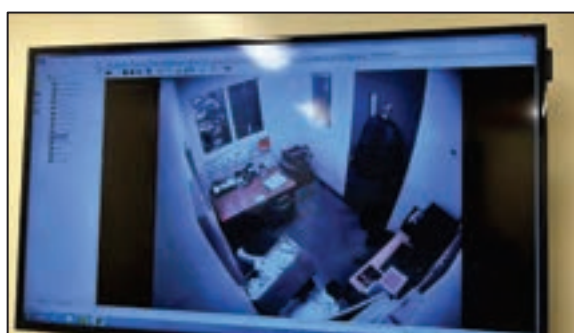


Figure 71 - Victor Video Surveillance Platform Camera Field of View

A myriad of fixed field of view cameras and pan-tilt-zoom (PTZ) cameras were observed with no verification made that PTZ cameras are programmed to return to a home position once manual use has been completed. It is assumed that the PTZ cameras are not used to track and monitor area activity as there is no physical monitoring of cameras across the district from either local or centralized location. Camera placement is ad-hoc with no consistent application of cameras at areas that have access control installed to support an alarm event-based camera call-up interface. Positioning of cameras to monitor emergency call stations is not typical. Parking lots also lack video surveillance



coverage and license plate recognition cameras are not deployed anywhere across District campuses to identify vehicles that should not be allowed access to District space.

Monitoring and Management

Ability to monitor video surveillance cameras cannot be achieved from a central location as the current topology of the system does not support a centralized management approach. Individual campus access control systems administrators do not have permissions to view cameras, and general understanding of who has visibility of cameras is inaccurate with a common understanding that district police have access to all cameras. This is not the case with district police at RCC able to call-up viewing of the Verkada cameras installed at the Facilities Department and Cashiers Office only. Challenges were observed with the remote Verkada login process, as infrequent use resulted in the user login information being forgotten impacting ability to call-up cameras on the mobile application. Viewing of the Victor platform cameras in most cases requires access via a client monitor/workstation usually located in the same data room where the associated NVR is located. Local viewing rights of cafeteria cameras is restricted to the person of authority at each campus. Direct access into the local NVR video storage and ability to monitor active cameras in real-time is available through standalone workstations. Again, disparity in video recording retention is apparent with some system users confirming 10-days availability on their NVR and others assuming over 30-days is stored. Training of system end-users is lacking, and knowledge of system performance capability is not known or understood.

The downtown Riverside Police Department Parking Services Office located on level one of the parking garage has a monitor that provides visibility of all video surveillance cameras installed at the District Office, Henry W. and Alice Edna Coil School for the Arts, and the Culinary Arts Academy. The assessment team are not aware of any other district police video surveillance monitoring stations.



Figure 72 - Riverside Police Department Parking Services Office Monitor

Alternate Video Management Systems

As identified the American Dynamics Victor video management solution is the predominant system in use across all district facilities with varied levels of software versions applied. Alternate solutions are either in early testing (i.e., Verkada) or have been fully deployed and are operational at local sites only (i.e., Panasonic iPro at the Facilities Department at MVC). As with recommendations regarding access control, evaluation of alternate solutions in comparison to a potential upgrade and refresh of the American Dynamics Victor platform is recommended in a



controlled manner. Challenges with localized deployment of multiple systems includes additional administration burden, procurement inefficiencies from a cost negotiation perspective, potential lack of integration with other existing security electronics eco-system components, and additional training required to educate systems users on how-to-use. The current security program lack of ownership provides opportunity for local campuses and buildings to deploy their own preferred system without reference to any district governance that mandates approved systems use. Other systems may provide additional benefit to the district, this review and evaluation process should occur in conjunction with an access control review to ensure that a fully integrated enterprise solution is utilized by RCCD improving the safety and security program.

Summary

Video surveillance is similar to the access control system regarding system age, performance capability, and topology. The American Dynamics Victor platform is capable of seamlessly integrating with the existing CCure 9000 access control and DMP intrusion detection systems. It should not be immediately overlooked but as suggested evaluated as part of a wider overall security electronics system review process. The current use of video is managed on an ad-hoc basis by those who have permission to view camera stream and stored video. District IT have minimal involvement post provision of network connection and installation of firewalls. IT are not responsible for the network hosted systems, and issues with video surveillance are routed through work orders to the local facilities departments. The current use of video surveillance fails to provide significant benefit to the RCCD safety and security program. Current technologies provide ability for greater visibility of activity with newer more advanced cameras, and lack of design standards result in gaps regarding visibility of activity at known areas of issue.

Recommendations:

The district should establish a standardized protocol for the installation of surveillance cameras at all RCCD campuses to ensure consistent application across all college premises, based on building function and areas of pedestrian and vehicular movement. Criteria such as camera placement, video frame rate, resolution, and retention duration should be carefully considered as integral components of this standard. Notably, the current video storage duration of 30 days, while assumed by many, remains unverified.

The primary objective of this standardized approach is to deliver practical and cost-effective protective measures against a diverse spectrum of potential threats through the disciplined and uniform deployment of security video surveillance technology. Incidents can be categorized as either "high impact, low probability" or "low impact, high probability" events. For instance, the surveillance system may facilitate remote verification of after-hours incidents detected by the intrusion alarm system or by video motion detection feature set capabilities, ranging from routine activities such as persons using the tennis courts at RCC to infrequent but high-impact occurrences such as the concealment of contraband on campus for later retrieval. In both scenarios, consistent surveillance, detection, and response protocols are applicable, delivering a comprehensive and reliable security framework across all campuses.

It is recommended to consider the following components when setting initial goals for future video surveillance system operations:

- Standardize on security video surveillance application across all RCCD locations, system type and general camera placement creating baseline expectations.
- Ensure system compatibility and integration with other electronic security components, including intrusion detection and access control.
- Minimize operational service and maintenance costs.
- Establish minimum equipment standards. such as camera types and characteristics
- Develop a comprehensive and future-oriented plan to steer upgrades and expansions.

Benefits of a standardized districtwide video surveillance system:

- Provides live and recorded video images of activity at each campus and facility.
- Provides forensic evidence from recorded video images.
- Provides capability to audit compliance with policies and procedures.
- Provides capability to remotely view activity at a campus or facility.
- Provides recorded video images that can be used for Faculty and Staff training exercises.

System Requirements

The American Dynamics video surveillance system would benefit from a centralized architecture approach. This would involve streamlining the existing provision of on-premises Network Video Recorder (NVR) servers to a minimal quantity based on storage needs determined by a new retention policy. These NVRs would be housed within secure, climate-controlled data rooms. A single management server would serve as the access point for authorized video users to view or retrieve video data from NVRs that they have permission to access.

Centralizing the video solution provides cost efficiency by reducing the amount of equipment required to store video, as well as reducing points of failure, maintenance, and service costs. It helps maintain security protocol compliance by supporting more efficient oversight and management. Centralized management also allows for consistent application of system features and analytics across the district. Restricting the number of people with administration access and providing audit trails of the management server increases visibility and accountability for activity.

To ensure operational efficiency, authorized personnel should have the capability to remotely access, view, archive, search, and perform administrative and management functions on any device with access to the American Dynamics (or other platform) through an online web portal. By implementing proper programming, system configuration, and management of encryption, access rights, access levels, and passwords, along with the enforcement of effective policies and procedures, the district can establish a robust enterprise-level on-premises system.

It is also important to establish standardized network cabling practices for security system network devices, including guidelines for cabling manufacturer, color, labeling, testing, and termination. Additionally, it is



recommended to ensure that network patch panels, patch cables, switches, routers, and communication protocols adhere to IT standards. If these standards are not already in place, it is beneficial to formalize them in coordination with Division 28's standards development.

To effectively manage video data, the district should seek legal counsel to determine the necessary video retention period based on state or local regulations. It is important to incorporate this retention duration into the official policies and procedures, system programming of video retention should be no-more or no-less than that defined. Additionally, documenting the recorded frame rate, resolution, and preferred recording option i.e., continuous or on motion detection will assist in accounting for server data storage needs during the planning of system upgrades or new installations.

To ensure the effective implementation of districtwide video surveillance, it is essential to have the necessary resources, support, management structure, and infrastructure in place. Key considerations to evaluate may include:

- Data network infrastructure
- Adequate electrical power and HVAC infrastructure
- Adequate controlled physical space for equipment
- Architect/Contractor/Consultant project design team
- Security electronics manufacturer/vendor involvement

Camera Considerations

It is crucial to select specific camera models that align with the unique performance requirements of the intended field of view. When determining the camera types for installation locations, prioritize performance criteria over the selection of specific camera makes and models. By adopting an approach to camera equipment selection based on functional categories, it is feasible to utilize equipment from diverse suppliers, as necessary.

A video surveillance camera/system performance criteria selection process may consider benefits including:

- Allows different cameras to be proposed and utilized on various projects while ensuring consistency and compatibility.
- Camera makes and models constantly evolve as vendors change devices and offer new product lines; basing device selection on performance criteria avoids specifying obsolete models.
- Take advantage of discounts and offers where possible without diminishing camera capability.
- Certain designer, vendor, and/or contractor team members may be able to propose specific camera makes and models based on their experience and knowledge which could be superior and/or more cost effective to the basis of design cameras.
- Allows camera "form factors" such as size, color, and visible profile to be adjusted for specific installation locations to improve aesthetics.

It is advantageous to avoid using cameras from a wide variety of manufacturers. This can reduce the complexity of maintaining different licensing and firmware. Therefore, a good strategy is to select a few pre-approved



manufacturers, such as Tyco, Axis, Hanwha Techwin, and Panasonic, to fulfill each performance requirement as needed. Reducing the broad range of camera manufacturers devices currently installed should be supported by identification of approved products only within Division 28 standards.

To ensure effective installation of exterior cameras, it is recommended to place them on building soffits and overhangs or use a wall-mount bracket arm for better cable routing into the nearest network equipment room. Although remote installation on poles or other structures is a possibility, it will necessitate additional conduits or cabling pathways to support the exterior camera cabling. It is important to note that a fixed field of view wall-mounted camera cannot provide a view back down the wall on which it is mounted. For example, if a hallway camera is wall-mounted, it cannot offer a view back down that same hallway. In such scenarios, it is advisable to ceiling-mount or wall-mount the camera at the 'T' at the end of the hallway to achieve an unobstructed view straight down the wall and back down the hallway.

Correct selection of camera types and their use in the appropriate locations²⁰ is important and key to maximizing the performance benefits that video surveillance can provide the districts security program. The following brief descriptives of varied camera types and typical areas of application should serve as a basis for developing and formalizing a security electronics device placement matrix.

Examples of camera types and their suggested applications are:

Exterior Fixed – Megapixel or 180/270/360 Degree Multisensor

- Exterior areas such as large open parking lots or quads with views unobstructed by trees or other obstacles
- Coverage of large exterior areas

Exterior Pan-Tilt-Zoom (PTZ)

- Exterior areas where events will host crowds or gatherings including stadiums, swimming pools, and parking lots
- Real-time live active use by authorized personnel

Exterior Fixed – Infrared Illuminators

- General exterior views such as parking lots and open areas with insufficient exterior lighting
- Active LED infrared illumination for nighttime surveillance

Interior Fixed – Microdome

- Interior corridors and other interior areas with even lighting and without an exterior window or door in the view (to avoid bright exterior light bloom in the view)
- Discreet camera size and installation

²⁰ [A Guide to Essential Types of Security Cameras and When to Use Each Type of Camera - Security Industry Association](#)



Interior Fixed – Minidome

- Interior entry lobbies and other interior areas with challenging lighting conditions such as an exterior window or door in the view
- Wide Dynamic Range (WDR)

Interior Fixed – Megapixel, 180/270/360 Degree Multisensor

- Interior of large buildings such as libraries, theaters, and gyms
- Coverage of large interior areas

Cloud-Based Solution

The district is currently using, as documented, an aging on-premises video surveillance solution. Considering the potential benefits, cloud-based solutions could provide a more efficient approach to video surveillance implementation compared to the traditional NVR model. Several cloud solutions including the currently trialed Verkada solution offer direct device-to-network viewing and system management by web portal eliminating NVRs providing edge device storage efficiency. Other commonly perceived benefits of cloud-based video management systems include:

- Ease of access to video stream from anywhere with an internet connection including use of mobile applications. Convenience of accessibility supports flexibility or access and eliminates constraints found with on-premises systems that do not utilize mobile applications.
- Additional scaling of systems is easily achieved simply by adding a device licensing cost for storage.
- Initial lower financial output as no on-premises metal box NVRs are required for storage.
- Automatic updates can be pushed out across all edge devices without additional programming through a server.
- Flexibility of movement of cameras from location to location without any requirement to direct network communication of video stream to an NVR. Simple network switch connection and internet access is all that is required.

Prior to reaching a decision, it is imperative to meticulously assess the operational costs associated with a cloud-based system in contrast to the conventional on-premises NVR solution. Some factors to consider may include:

- Network infrastructure and bandwidth provided by the district are required to support 24/7 upload of camera data. For large scale campus implementations, investment in this infrastructure could be significant.
- Cloud-based systems may have monthly or yearly recurring video storage costs that are an operational expense that must be budgeted. If the district stops paying the monthly fee, recording of video may stop.
- Cloud-based storage belongs to the video storage systems provider and is not under direct ownership of the district.
- There is a risk that video may be unavailable when required if there is a loss of service or communication path to the storage provider.
- System lifespan cost should be calculated to identify where the operational cost of operating a cloud-



based system for a specific number of cameras exceeds initial capital expenditure costs of a district-owned NVR storage solution for the same number of cameras.

Summary

The historical approach to installing cameras to campus and buildings on a project-by-project basis without governance or review with a security program owner should cease. Informed, and governed decision making should drive the application of future video surveillance system refreshes and new camera installation. Enterprise level systems administration should be created to provide a one-stop-shop point of contact regarding systems management, maintenance, and access. Ability for local visibility of camera activity is encouraged with live streaming monitors installed at key building reception areas as identified within the individual site reports, providing ability for building occupants to passively monitor activity on the public approach to buildings. Collaboration with the district police is encouraged by engaging their perspective and thoughts on how the deployment and provision of access to view live video streams may support their role function. Evaluation of the current platform and alternate options is recommended, creating a new baseline position for existing system refresh or new system deployment should be an action item performed in conjunction with access control system evaluation.

Visitor Management

Findings:

Visitor management processes appear lacking across RCCD campuses and administrative buildings, with exception of the Early Childhood Education Centers at RCC and MVC who require visitors to make themselves known at the front reception areas. The assessment team did not encounter any other visitor management sign-in processes across college campuses. Arrival at the District Office requires notification made to the person visiting by the reception desk, the contact then meets the visitor in reception prior to accessing the secured space. Visitor management procedures are not driven by district policy and general reference to visitors is limited to signage that indicates visitor parking spaces only.

The lack of visitor management processing can present vulnerability and risk to people management with inability for local floor and building captains, and first responders to utilize an attendance record to account for all persons in an emergency event (i.e., fire or earthquake). Secondly, without visitor management there is no capacity for visitors to be validated prior to entering RCCD buildings; this is a bigger issue at campuses where access to most buildings is easily achieved as main points of entry remain unlocked and open on schedule. The current visitor experience encountered across RCCD campuses and administrative buildings found that there are no “special measures” in place i.e., verification of identity, or issuance of photographic visitor badges in place. Furthermore, the assessment team were challenged little regarding who they were, what they were doing, or if they required assistance by other campus users; with exception of being challenged by the custodian team at NC during the evening lighting assessment, other approaches did not occur. This indicates a culture that is not fully tuned-in with the benefits of identifying visitors as known authorized persons who are approved to be on campus, or within certain buildings.



Visitor management can be challenging to implement across community colleges due to the open public nature accessibility into buildings as found at RCCD. Strong visitor management requires supplemental measures such as clear instructional and directional physical signage, wayfinding, building identification, and visitor management system administration personnel, all to be in place if to be successful. A streamlined check-in and check-out process is required for efficiency and to avoid frustration from the visitor perspective that may cause avoidance of the process at future visits.

The existing RCCD security electronics access control platform CCure 9000 has capability to support visitor management at all RCCD locations either by using local self-service visitor kiosks, or by enabling hosts to directly create and manage their own visitor appointments. The ability to centralize visitor management and empower staff and faculty to administer and manage visitor appointments, reducing potential additional resource headcount and cost is an available option. Procurement of additional software licensing, development of policy and procedures, and provision of training would be required if this were a consideration for RCCD.

Recommendations:

When evaluating the possible implementation of a formal visitor management system there are several key challenges that RCCD should consider, some challenges also provide benefits:

Operational Challenges:

- High visitor traffic: Community colleges experience high volumes of visitors due to open enrollment, diverse student populations activities, and community outreach programs. The diversity of campus use encourages a mass populous which presents a challenge to manage, it does however positively enhance natural surveillance. This mass populous also presents an opportunity to showcase the college's welcoming environment.
- Multiple access points: Campus layouts with numerous entrances call for complimentary solutions to streamline visitor control and monitoring. As described prior, signage and wayfinding are key to directing visitors to registration points.
- Balancing security with accessibility: Finding ways to maintain a secure environment while ensuring easy access for visitors can lead to potential unintended access vulnerabilities. Controlled building access can restrict unauthorized entry but may compromise the culture and welcoming feel intended. It is important to establish visitor sign-in points at locations that are easily accessible for from visitor access points on campus.
- Staffing limitations: Leveraging technology and training initiatives can enhance visitor management despite limited personnel. The existing district access control system supports the ability to implement a visitor management module that allows hosts to manage their own visitor appointments, with information stored centrally (if a centralized access control system is adopted).
- Technology integration: As above integrating a visitor management system with existing campus security electronics infrastructure and software modernizes operations utilizing security electronics to support and improve security operations efficiencies.



Cultural Challenges:

- Open campus culture: Embracing the open campus culture while ensuring safety through workable design and operational policies can enhance the visitor experience. Each campus may have its own cultural needs that require consideration to visitor management roll-out.
- Visitor expectations: Communicating the importance of registration and identification can help visitors' awareness of the college's commitment to safety and security. Visitors are to be active participants of the safety and security culture and should be expected to participate appropriately if they wish to visit campus or other district facilities.
- Staff and Faculty buy-in: Provision of comprehensive training and aligning procedures with the college's values can foster staff and faculty support for visitor management efforts. Staff and Faculty engagement should require minimal time outlay with benefits of engagement and participation front and center of training. Participation should not be perceived as a chore, otherwise the process will never move forward with positivity.

Financial Challenges:

- Budget constraints: Localized budgetary funding may cause restriction and delay on potential procurement and roll-out of a visitor management system. If a “bolt-on” module to the existing access control system is considered an option, central district funding is recommended. Localizing funding may exasperate further the inconsistent levels of software and service level agreements in operation, that cause inconsistency of systems use and support. Visitors should have the same experience at all RCCD locations, and central district management, and ownership is critical to successfully achieving this.

Key to successful visitor management roll-out is the provision of staff training, development and distribution of procedural guidelines, and validation that all shared personal private information provided by visitors is managed and protected by data privacy and protection measures. Implementing best practices for data privacy and protection can reassure visitors about the security of their information. By addressing and overcoming the challenges described, the district can develop an effective visitor management approach that will enhance the safety of, and the overall visitor experience.



Emergency Telephones

Findings:

Emergency telephones are distributed across all District campuses and within the downtown Riverside parking structure in different form factors (i.e., towers and or wall mounted), located primarily at parking lots, and found in different conditions of operation. It should be noted at the outset that emergency phones and the non-operational state of many was a point of conjecture for some stakeholders interviewed. There is concern that emergency telephones that require maintenance and repair and are non-operational present risk and liability when, if needed, they do not provide immediate communication capability. Emergency phones are a vital and critical communication tool that should be 100% operational, frequently tested, and dependable for use when needed. The public-facing optics of equipment that is non-operational, in need of repair or simply damaged through environmental conditions has a negative impact on campus users and reflects poorly on the security and safety program of RCCD. The phones are a potential lifeline tool that should function correctly at all times and be installed with a consistent form factor and appearance to support easy identification and familiarity amongst campus users.

The positioning of emergency phones across district campuses, as stated, are primarily within parking lots and garages. Phones are provided throughout pedestrian walkways. However, the lack of consistency in unit form factors and condition, with lack of location of phone locations displayed by signage, it is challenging to easily identify them. Additionally, many blue strobes were observed as lacking power or needing the bulb changed as the predominant state of campus emergency phones was lack of illumination of the strobes 100% of the time. Typical operational best practice is that the blue strobes are always illuminated and then they strobe when a call is activated. Ability for remote visual awareness of locations where calls are being made from is not possible as video surveillance cameras are not deployed to view the call stations, and integrated video cameras are not included within the call station units. Communication to the District's access control system is not present. There is no means of notification for the activation of an emergency telephone other than at the receiving call agent at the County of Riverside Sheriff's Dispatch Center.

There is no communication call stations-standard applied to district facilities, and most units have single emergency call buttons with no button available for general assistance calls to be made. Provision of instructions on how to use the call stations and information on where calls are received is not provided. Several call stations at MVC did display the location of the phone on campus with a campus map present. These are exceptions to the norm.



Figure 293 - Emergency Call Station with Campus Map at MVC

At the time of assessment several emergency call stations were out of order at each campus. Reasons provided for this status include damaged communication cable, cellular upgrade required, broken call button, low volume, and lack of communication. Disparate manufacture call stations in use adds additional maintenance and management challenges. Call stations by Trigon and GAI-Tronics were end-of-life and in the case of Trigon they are no longer in the marketplace rendering parts and replacement units difficult, if not impossible to source.

Emergency call stations known to be out-of-order include:

Moreno Valley College

- Parking Lot E
- Parkside Complex 6

Norco College

- Lot A East
- Lot A West
- Lot B North
- Lot B South
- Lot C North
- Lot D (Near CSS)
- Activity Center
- Soccer Field South
- Soccer Field North

Riverside City College

- Quad 2nd Floor N/W QD-21
- Health Services Vendor Road
- Parking Structure 3rd Floor N/W
- Evans Field East
- Evans Field West
- ECEC Lot M
- Nature Trail West
- Nature Trail Middle
- Nature Trail East
- Parking Lot J
- Parking Lot K
- Parking Lot N
- Parking Lot U
- Parking Lot Q
- Lovekin Complex L10
- Parking Lot E

Examples of some of the different form factors, operational state and manufacturer units in use are illustrated in the following images. Placement of units such as exterior rated units within interior spaces demonstrates a lack of standardized approach supported by governance reference documentation. Equipment appears to have been

installed as campuses have evolved with no consideration for existing conditions, resulting in disparity in form factor and performance features of each unit type installed on a project-by-project basis.



Figure 304 - Code Blue Wall Mount Call Stations w/ Independent Blue Strobe

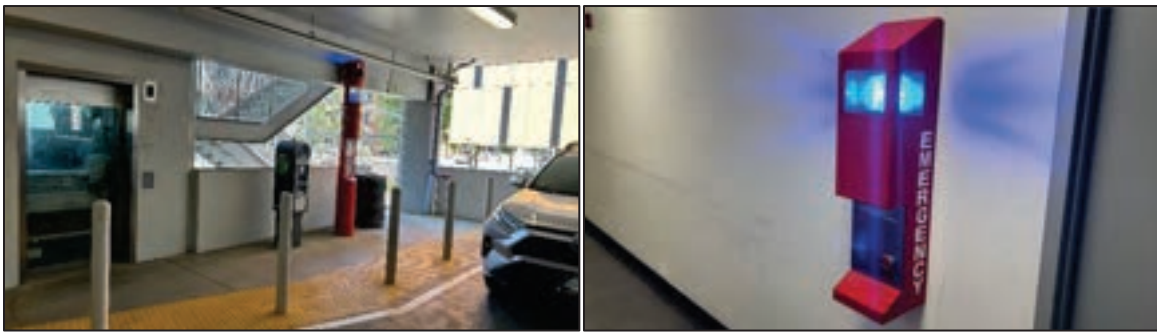


Figure 315 - Code Blue Tower and Wall Mount GAI-Tronics Call Station w/ Built-in Blue Strobe



Figure 326 - Trigon Wall Mount Call Station w/ Independent Blue Strobe

An item of note at NC was the installation of call station units that appear to protrude beyond 4” from the wall. The 4” protrusion is non-compliant with current American with Disabilities Act regulations that state that “Protruding objects shall comply with 307. 307.2 Protrusion Limits Objects with leading edges more than 27 inches (685 mm) and not more than 80 inches (2030 mm) above the finish floor or ground shall protrude 4 inches (100

mm) maximum horizontally into the circulation path.”²¹ Reference Figure 74, for approved protrusion allowances, future security design standards should consider protrusion limitations when identifying approved equipment types.

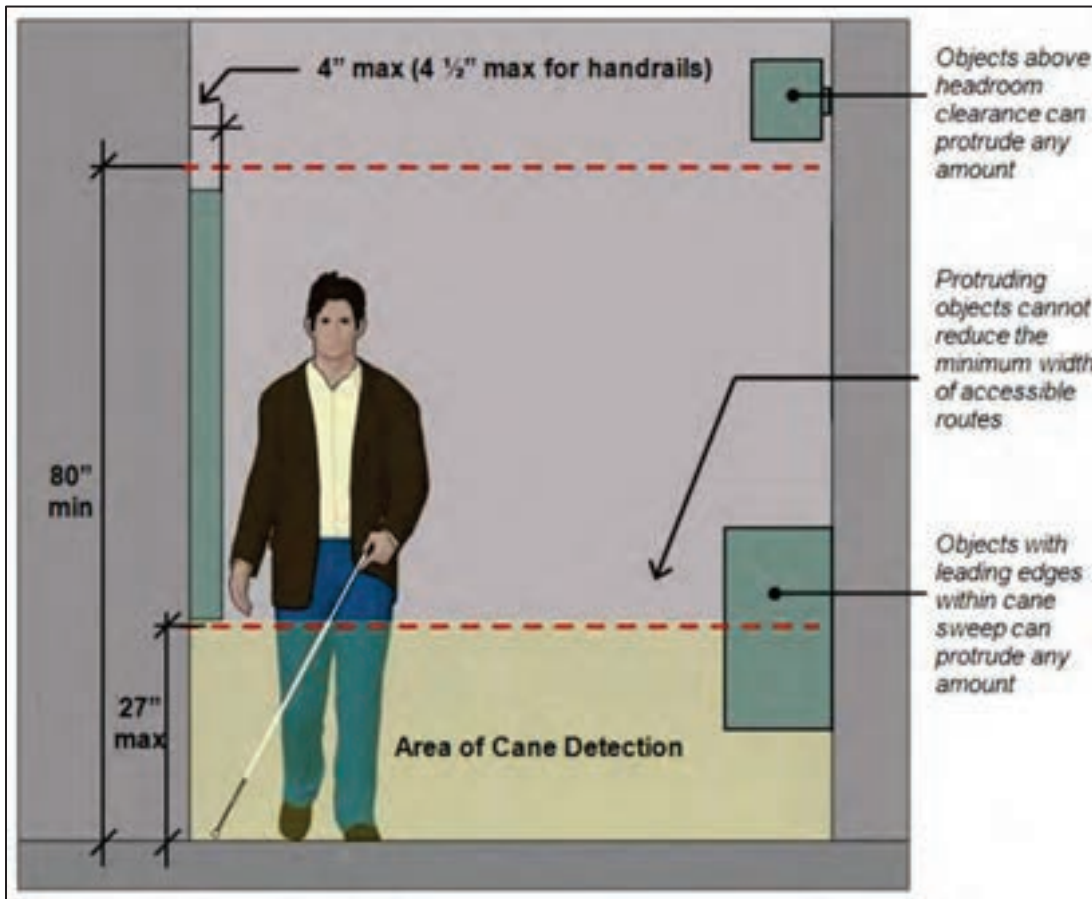


Figure 337 - ADA Protrusion Limits "Shoreline" Wall

The current inconsistency in product type, location of placement, operational state, inability to provide camera call-up, ease of identification, end-of-life and non-operational condition, and lack of ease of identification of emergency call stations is concerning and potentially problematic if a campus or facility user requires immediate assistance and a call cannot be successfully placed. A comprehensive review and overhaul of emergency call phones should be considered.

Recommendations:

The age of the cell phone has presented alternative options for community colleges, i.e., mobile applications, to be used as a means of direct communication between campus and facility users and call/incident responders. There is

²¹ [Chapter 3: Protruding objects \(access-board.gov\)](http://access-board.gov)



no current defined best practice standardized approach regarding emergency call stations and their utilization within community colleges, rather it is each college districts security culture that will determine their use. Devices identified and known as out of order should be fixed, as these units offer a potential lifeline to campus users and should not sit for any period time as non-operational. Non-functioning devices that are not to be repaired should be removed as there is risk associated with the expectation of operation. It is critical that life safety equipment be operational to function as expected when called upon.

It is recommended that the district identify and standardize upon both an edge communication unit and form factor for deployment of emergency phones. Technology applied, form factor (i.e., towers and wall mount), use of strobes, and color are all critical and should be consistent across all RCCD campuses and facilities. Newer technology supports integration with mass notification platforms via Session Initiation Protocol (SIP) and also provide notification of calls to several monitoring outputs through alarm event trigger programming (i.e., access control notification and camera call-up), supporting efficient response.

Evaluation of device placement is also encouraged. The ability for campus users to easily identify emergency call phones from within the main pedestrian walkways and gathering areas should be considered. An overhaul of the existing emergency phone deployment is recommended with supporting operational protocols created, user information displayed locally, and response protocols documented with written policy and procedures. Frequent, scheduled testing of units should be documented, and liaison with the County of Riverside Sheriffs Dispatch Center encouraged to define, review, and adjust as appropriate to ensure call response protocols provide efficiency to call activation response.

Why continue to provide emergency call stations?

Emergency phones as indicated within the report are seen as non-essential at some higher education institutions with the widespread availability and use of mobile phones by the populous mass, generating an increasingly common consideration for removing emergency phones. Other education institutions are continuing to supplement the importance of emergency call stations as illustrated by recent investment at UC Davis with \$675k earmarked specifically for emergency call boxes.²² Removal of emergency call stations is not recommended as there are a number of factors that mitigate risk of the potential reliance upon cell phones and enhance the security posture of a campus by emergency phones being present:

- **Reliability:** Analog or IP devices, hardwired, provide reliability of communication that should be confirmed via regular performance checks that cannot be confirmed for individual campus end-users cell phones. Cell tower dead spots present risk to the college if in need of emergency help a call cannot be made.
- **Visual deterrent and accessibility:** The devices provide visual presence that help is available and can be used as target points to request help rather than the alternate fumbling for a cell phone and having to dial a number. The simplistic but effective call stations provide one button call activation and flashing strobe annunciating to others that a request for help is being made.

²² [UC Davis Invests in Additional Security Improvements | Finance, Operations and Administration](#)



- **Immediate response:** No reliability on subscription to mobile applications. Again, direct means of communication versus reliance upon a cell phone and third-party application. Risks associated with applications include subscription failure, licensing maximization and reliance on cell service coverage.
- **Systems interface:** The units can interface with other systems to provide situational and response awareness through input to other systems i.e., video surveillance.
- **Power of presence:** Their physical presence alone can provide end-user comfort and often transmits a sense of safety and security through them just being there. Positive impact for new students who may factor safety and security into their review and selection process when identifying where their next place of learning will be.

Form Factors, Tower, and Wall Mount

Standardization on form factor of both tower and wall mount emergency call stations is recommended. The district currently deploys devices manufactured by Code Blue across several locations including the downtown Riverside parking garage and a single unit at NC in the Operations Center. Code Blue are a leading manufacturer of emergency communications solutions and a solid reputable organization, they offer products of varying power requirements, communication capability, and form factors. Standardizing on Code Blue should be considered, and potential form factors for tower and wall mount devices are suggested.

Towers

Subject to wider stakeholder engagement and desired communication options preferred by RCCD, Code Blue offers a wide range of product types with the CB 1-s and CB 1-w. Two options that provide comprehensive features that would meet the majority of operational considerations likely to be encountered. The CB 1-s provides communication through hardware, cellular, and IP wireless, powered by AC/DC and optional PoE. The CB 1-w offers cellular and IP wireless communication only but is powered by solar offering unrivalled flexibility of installation in areas that have challenges with providing power, or require significant trenching costs to provide communication cables etc.

It is suggested that overhead camera mounts be installed providing ability to receive real time awareness of activity at the location of call placement through integration with video surveillance. Code Blue also offer audio paging units that sit on the top of both the CB 1-s and CB 1-w towers that should be considered as part of any mass communication public address roll out.



Figure 348 - Code Blue CB 1-s, Video Camera Extension, and CB 1-w

Wall Mount Units

As with the tower options Code Blue offers wall mount enclosure options, several with built-in strobes (preferred). The CB 2-a wall-mounted Help Point® has a sleek profile that is slim enough to be ADA compliant on any wall, it is a lightweight durable two-piece stainless steel construction unit that makes installation easy for a single person. A high intensity LED beacon/strobe and faceplate lights provide high visibility for the hands-free emergency speakerphone and makes it an excellent choice for parking decks, building entrances, exterior and interior corridors, and lobbies etc. The unit supports hardwired, cellular and IP wireless communication and powered by 12/24 VDC with PoE optional.



Figure 359 - Code Blue CB 2-a



All units presented can be customized in color and graphics as needed. Standardizing the emergency call station form factors will add a positive impact to the sense of safety and security across all RCCD facilities. Escalation of review of emergency call stations should be a priority action item.

Video Intercoms

Findings:

Dedicated video intercoms can provide the ability for communication between a public space and a secured space both visually and audibly, allowing the verification of person(s) requesting entry prior to granting them access. Additionally, the internal intercom feature typically found on VoIP telephones (not activated on RCCD campus phones) provides ability to turn telephones into intercoms with direct calling between phones, group calling, and wide area all-call broadcast.

Several dedicated video intercom units were observed across the district facilities including at the Library at MVC, and the Early Childhood Education Center, and Cashiers Office exterior entry at RCC. Several areas across the campuses with controlled access were identified as locations where video intercom would benefit the safety and security of building occupants on a daily basis or during heightened security times when shelter-in-place or lockout occurs. Some areas identified during the assessment that have the ability to verify and validate requested entry into a secure space without free ingress being available include:

Moreno Valley College

- Cafeteria delivery area
- Early Childhood Education Center main entrance
- Student Administration Services exterior opening that provides access to administration and executive offices

Norco College

- Kitchen delivery area
- President's Suite main entry into the reception area
- Engagement Center ST107

Riverside City College

- Administration Office Admin Wing Space 230
- Information Support Services entry opposite the Library
- Tech Center Network Room 214 exterior opening
- Building of Business Law Deans Suite
- Facilities Department main entry
- Tech B access opening to district staff space only
- Cosmetology Building main entrance



All areas are identified and further documented within the individual site observations and recommendations reports. Operational review of spaces is encouraged, as there are many areas that are equipped with access control that is unlocked on a schedule, always providing free ingress with no communication with the public side available if there is a need to lock and secure doors. Staff and faculty should be engaged as concerns were shared at some locations that the inability to identify persons requesting access to spaces prior to them entering presents a sense of unease and concern regarding safety and security.

External intercoms are also not installed at the downtown Riverside facilities or at the Norco Innovation Center. The downtown Riverside facilities are continually accessed by members of the public with no remote communication capability available if entry doors are locked and secured. Lack of intercoms also fails to provide staff with a communication means to notify building occupants that they require building access if they have forgotten access credentials, keys, or cell phones and are locked out. The lack of intercoms dictates that entrance points be physically viewed to verify and allow access when doors are locked and secured, rather than validating from a safe, remote vantage point. The rear entry to the Center for Social Justice and Civil Liberties building is outside of the secured delivery and parking area. This facility specifically is exposed to public access, and staff purposely raised concerns with the lack of visibility of activity in this area. A video intercom would alleviate these concerns.

Recommendations:

It is recommended that the District review locations where the ability to restrict public and secured space accessibility would provide benefit to the immediate safety and security of local building occupants. Consideration of installation of IP (Internet Protocol) PoE (power-over-ethernet) video intercom door and master stations is recommended with integration to the access control system to allow remote release unlocking of doors as needed. The ability to verify visitors, other persons requesting entry, and maintain a controlled secured space is an immediate need of the downtown Riverside facilities.

Modern IP-based video intercom units provide the ability for door calls, when activated, to be routed to mobile devices (i.e., cell phones), providing flexibility for the persons receiving calls to perform tasks away from the master station location. Call routing is also a feature of intercom systems; however, some end-users feel their security may be compromised if they do not feel comfortable with their number being publicly issued. Voice-activated video door intercoms eliminate these concerns with audio utilized to route calls to appropriate persons. It is recommended that 1-way video intercom systems be considered reducing the public side ability to see the call receiver.

Integration with the access control and video surveillance systems provides wider visibility of activity visually if the integrated intercom camera stream is programmed to pop-up within the VSS monitoring stations when a call is activated. When used in this way, intercoms become the first line of controlled interaction with building occupants from a restricted distance rather than directly face-to-face. District culture must be considered when implementing intercoms particularly as how they pertain to everyday operational use. Flexibility in consideration of operational use on a case-by-case basis is considered as there are several different use case scenarios that may support more frequent use at some locations than others.



The use of the telephone intercom capability on wall or desk-mounted telephones across the district colleges is encouraged if telephones are deployed as typical within all classrooms and of newer technology that supports this feature. Telephone intercoms provide cost efficiency and scalability of communication performance capability when using phones that already support this. The ability to instantly communicate with others using defined user call groups offers immediate connectivity with multiple users without a need for inputting separate contact numbers that may cause delay to a request for assistance. The district office and adjacent downtown Riverside facilities should have ability to easily communicate with each other via telephone intercom if available on existing handsets. This would provide redundancy to other communication tools (i.e., radios).

Public Address

Findings:

The use of Public Address (PA) systems both internally and externally across RCCD is limited to the MVC Dental Center audio only (internal system), and the NC (external only) siren system, with ability for pre-recorded messaging to announce. No other public address system in use was known by chaperones at the time of assessment and speakers indicating that they were part of an operable public address system were not identified. Audio and visual notification systems are often fundamental to emergency response measures, with their performance important in events that require specific instructions to be given. Areas such as the NC Sports Complex would typically be areas where public address speakers are installed locally as an immediate means for providing communication to large gatherings of people.

PA systems are often seen as indispensable means for quick dissemination of critical information during events such as fires, natural disasters, and security threats. Advancement of technology has seen transition from older analog systems to newer network-based systems that provide remote management and supervision. Routine testing is important to ensure that communications are routinely made with intelligibility of communication confirmed. NC perform quarterly testing of the American Signal Corporation, Central Station Controller CSC-960²³.

The NC CSC-960 unit is managed from within the Operation Center and is secured within a cabinet. *The Central Station Controller 960 is a Status Encoder and siren control unit. The CSC-960™ command and control system is designed for ease of use and simplicity of activation; inserting and turning the key unlocks the control panel and pushing the appropriate button activates predetermined sites with pre-programmed audible alerts.*

The CSC-960™ is equipped with battery backup to provide a minimum of eight hours of continuous operation in the event of main power failure, to ensure the utmost reliability of the siren controller. This siren control unit has a key lock to secure the keypad; four LEDs to indicate power, status of the RF carrier, Cancel, and a spare function; and ten programmable function keys on the face of the unit. The keys of this command-and-control system may be programmed to execute a variety of activation commands across the managed sirens.

²³ [Command and Control Systems | Siren Controller \(americansignal.com\)](#)



Scripted messaging pre-programmed within the system at NC include:

- System Test
- Active Shooter Warning
- Severe Weather Warning
- Tornado Warning
- General Evacuation/Undetermined Threat in Area
- General Announcement Notification
- Emergency Message Notification
- Child Abduction/Missing Notification
- All Clear

Lack of public address fails to support notification of lockdown or shelter-in-place at spaces where electronic locking of doors may occur without notification i.e., restrooms at MVC adjacent to the Dental Center, and areas with no other means of communication than cell phones such as the Catherine S. Huntley Gymnasium at RCC.

Emergency call station towers provide infrastructure to support placement of speakers, no utilization of existing call towers for mounting of PA speakers occurs.

The lack of standardization in placement of telephones within district classrooms (RCC and MVC typically have no classroom telephones), requires students to remain subscribed to the RAVE Alert emergency communication to receive push notifications if an emergency communication is issued. This presents risk liability that the provision of communication via a PA would mitigate. Assumption that cell phones are powered on, off-silent, and on-the-physical person of the owner of all students is potentially risky should a student walk into an incident due to not receiving a communication. Audio and visual PA would again mitigate against vulnerabilities in the mass communication protocols if deployed, providing a means to communicate internally and externally of campus buildings simultaneously.

Recommendations:

It is recommended that the district consider installation of internal and external audio and visual PA across all its facilities. The reliance upon the RAVE Alert emergency communication as a primary means of mass communication approach has flaws. As discovered during site assessments several persons interacted with, advised that they had opted out of the alert system through lack of understanding and training regarding its intent. Such action diminishes the immediate reach-out audience that RAVE Alert speaks to, and a secondary more static and localized communication system encouraged. Furthermore, several persons interacted with were uncertain of what the RAVE Alert emergency communication is.

Immediate review of the performance capability of the NC American Signal Corporation, Central Station Controller CSC-960, should occur to determine if its current operational use continues to meet NC needs and those of other district campuses and buildings. Internal and external annunciation capability should be determined. Alternate solutions may be considered if the CSC-960 is not an amenable solution for use elsewhere.

Leading alternate solutions such as the Singlewire Software Informacast²⁴ platform is an expansive communication platform that supports input from multiple devices and other systems with ability to then transmit communications through a wide array of tools and interfaced platforms. The Informacast platform also provides ability to unify communication channels into a single “pane of glass” to manage and administer communications.

The system supports mass text notification similar to how RAVE Alert messaging is currently used but through one platform that also supports indoor and outdoor speakers, digital signage, desktop computers, and mobile devices. Informacast also offers its own visitor management solution Visitor Aware²⁵ providing an alternate consideration to the CCure 900 visitor management module, managed from within one pane of glass.



Figure 80 - Informacast Mass Communication Solution

Centralized management of a PA network-based solution is recommended, with local access to the system provided with ability to use locally determined by local administration and key stakeholders, with access managed through permissions controls such as access code issuances etc. Wider distribution of systems access codes should be supported by user protocol and procedure, misuse should not be accepted. Use of a network based centralized solution provides cost benefits over traditional analog units with no requirement for localized head-end equipment, reduction in maintenance upkeep, ability to interface newer technology solutions where install challenges occur, and systems monitoring support’s ability to monitor tampering and identify when systems components may be down.

Of critical importance is the intelligibility of any communication made audibly over the PA system. The industry has developed a measurable technical standard for grading the intelligibility of a sound system within a particular space called “STIPA,” which stands for “Speech Transmission Index for Public Address.” Using a specialized signal generator (called a “talk box”) and a portable sound meter/acoustic analyzer, a STIPA rating can be determined for an “acoustically distinguishable space” (“ADS”). This is a space – enclosed or not – with acoustic properties

²⁴ Singlewire Software Informacast

²⁵ [Visitor Check-In Software - Singlewire Software](#)



different from the adjoining spaces. A classroom is an example of a closed ADS. A corridor with no doors between two larger areas is an example of an ADS that is not physically enclosed.

Below depicts the STIPA scale:

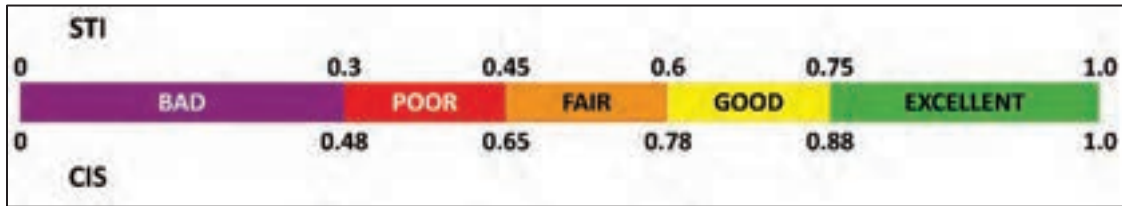


Figure 81 - STIPA (Speech Transmission Index for Public Address Systems)

An intelligently designed, conventional public address system is expected to fall between 0.45 and 0.6 on the STI (upper numbers) scale. The National Fire Protection Association's (NFPA) National Fire Alarm and Signaling Code (NFPA 72) considers an emergency notification system acceptable if 90% of the measurement locations within each ADS meet a minimum of 0.45 (fair) with the ADS having an overall average measurement of 0.50. The scale assumes the message broadcast over the PA is in the same native language as the listener. If the listener's native language is different, then the PA's performance is likely to be subjectively worse. Any future PA consideration should reference current NFPA recommendations for intelligibility of PA annunciation.

Radios

Findings:

Two-way radios are common in use across the district facilities with Facilities teams using them as their primary means of immediate communication. Radios provide communication using dedicated channels across large areas such as the individual campuses, providing a low cost-effective solution that does not rely on any cellular network for communication between handsets. Despite radios being a low-cost item, individual campuses procure their own radios with no district preferred manufacturer or model type identified as a standard.

In addition to the Facilities teams, radios are used by Floor and Building Captains, Grounds and Maintenance Teams, Custodians, Campus Safety Coordinators, Sports Complex Staff, Early Childhood Center Staff, Administrators, and others. It is understood that the District Police also have ability to listen in to certain communication channels, but the district radios do not allow for direct communication with the District Police. Emergency Operations Centers (EOCs) have dedicated radios with a communication channel set-up and ready for immediate use if needed. EOC radios at both MVC and NC were observed residing in charging bays.

Radios in general are robust, with inconsistency in manufacturer and model types deployed. A concern regarding radios observed at the MVC Early Childhood Center, was feedback provided by staff that the radios experience frequent intermittent failure. This is problematic as the operational expectation is that radios are taken by playground supervising staff as a means to request immediate assistance when overseeing playground activity. If they are non-operational ability to request assistance is diminished. Note at the time of this assessment radios

were not on the person of yard supervisors. These radios are also procured directly from an online shopping source and are not district or local college issued.



Figure 82 – MVC Early Childhood Center Radios

Robust SRcomm radios are used at NC with two different form factors in operation. The higher performance SRCOMM SR-D3U specification handheld radios are used on a day-to-day basis to support operations. The lesser performance feature SRCOMM SR-D1U radios are those that are used by the EOC. Dedicated channels are programmed for Facilities, Special Events, and Emergency Communications with several others available for general talk traffic. NC has established local operational guidelines that provide clear and concise instructions on “How-to” use the radios. This documentation is excellent and provides easy to follow reference material for radio users.

The radios illustrated at the Center for Social Justice and Civil Liberties are manufactured by Midland Radio and are used locally.



Figure 363 - SRcomm Radios at NC



Figure 374 - Radios at Center for Social Justice and Civil Liberties

Radio repeaters are in use across several campuses providing reinforcement to the transmittal of radio communications. In addition to repeaters, an Emergency Responder Radio Communication System (ERRCS) was observed at the newly renovated Building of Business and Law, at RCC. ERRCS, as the name suggests, is designed to ensure mission critical radio coverage for emergency services within buildings. Many jurisdictions enforce the code defined mandates for their deployment to provide reliable communication for first responders throughout the entirety of a facility including the critical areas such as pump rooms, utility spaces, and stairwells. Building materials can affect radio frequency strength, the Building of Business and Law consists of concrete block that significantly impacts communication frequencies. This location was the only ERRCS observed across the district buildings.



Figure 85 - Emergency Responder Radio Communication System (ERRCS) panel at the Building of Business and Law, RCC

The Emergency Responder Radio Communications System (ERRCS) is made up of:

- A donor antenna to receive off-air signals.
- A BDA (Bi-Directional Amplifier) to amplify the low off-air signal strength to a high output power.
- A series of cable and splitters to distribute the signal throughout the building.
- Service antennas to transmit the signals at the end of each cable run.
- A battery backup to keep the system running in case of a power failure.
- An annunciator panel to display the status of the ERRCS System and inform first responders if their radios will work within the building.



ERRCS is covered in both International Fire Code (IFC Section 510: Emergency Responder Radio Coverage) and in National Fire Protection Association, NFPA 1221 Section 9.6 (Two-Way Radio Communications Enhancement Systems). Both of these documents require that all buildings that do not have adequate radio coverage, which can be determined with a benchmark test, must have an ERRCS system installed to provide the required coverage.

Recommendations:

Continuation of radio usage is encouraged as they provide immediate communication amongst preset user groups delivering consistency in performance. The standardized issuance of radios to Floor and Building Captains is excellent. It is recommended that the district also standardize on radio manufacturer and model types. This would provide the district with a stronger position for procurement cost negotiations, deliver standard quality and operational performance experience across district facilities, and improve wide area communication with shared preset channels.

Existing self-procured radios at the Early Childhood Center at MVC should be replaced with district approved radios. Review, revision, and or adoption of the radio guidelines detailed at NC should occur and a standard user guide formalized through district board policy and communicated out. Review of preset communication channels should identify dedicated channels that support cross campus communication and communication with the District Police.

Telephones

Findings:

Use of telephones across RCCD campuses and administrative buildings follows in general, a simple distribution process; all office and workstations receive voice-over-internet-protocol (VoIP) handsets, classrooms do not receive a phone at all. There are exceptions to this rule most noticeably at NC where telephones have recently been reintroduced into classroom spaces. Concerning observation at NC was the removal of telephones from classrooms where they were reintroduced without any notification provided to the Safety and Emergency Planning Coordinator. Removal without notification may impact an incident response if an assumed means of communication is no longer available when called upon.

VoIP handsets typically observed are NEC Univerge DT700 series which have been in operation since pre-2010. These handsets are near end of life and lack sufficient performance features to support mass communication needs with intercoms that are unavailable. Newer NEC Univerge DT800 series phones were observed within office spaces and open staff workstations. The DT800 series includes models like the DT820 IP Entry-Level Phone, which offers a monochrome 3.5" or 4" LCD display, and the DT830 IP Desktop Phone, which features a full-color 3.5" backlit LCD display. These phones are designed to be customizable to fit the specific needs of each employee within an organization, supporting a wide range of applications to improve efficiency and productivity. They also come with features for the visually impaired, such as audio key action feedback and large character display.



Figure 386 - NEC VoIP Telephone Handsets (New and Old)

Provided telephone handsets appear to be used inconsistently regardless of office or classroom space, with cell phones being the preferred means of communication. The current VoIP telephone system supported by an NEC PBX²⁶ (private branch exchange) requires migration to another service provider as NEC have announced that they will no longer support systems after December 31, 2024. Consideration should be given to ensuring that existing hardware is compatible with any new digital PBX selected.

Traditional landline telephones are restricted to (as informed) one landline per campus. These Plain Old Telephone Service (POTS) lines are provided for single emergency communication phones and are used if loss of power to the network VoIP system. The only landline visually identified was at NC, the phone number displayed on the red handset (see Figure 84) was called and verified as still active. POTS lines typically remain as a means of backup communication in the event of loss of local network or wider cellular network outages. They are often seen as insurance for use in emergencies when cell towers may be overloaded with communication efforts and are seen as more reliable. Costs of maintaining POTS lines is increasingly expensive as fewer remain in operation. POTS lines are sunsetting. Post Federal Communications Commission (FCC) Order 19-72A1 directed that all POTS lines in the U.S. be replaced with an alternative service beginning August 2, 2022. Transition from POTS line also affects security electronics and life safety systems that have traditionally relied upon POTS lines for communication offsite to third-party monitoring stations.



Figure 397 - POTS Landline at NC

²⁶ [NEC To Shutter On-Premises UC Operations Outside Japan - UC Today](#)



Recommendations:

The need for the telephone system to migrate from the end-of-life NEC PBX to a new provider is critical to maintain basic communication capability. Conversion to a digital PBX is recommended as they provide improved cost efficiency, performance features, and scalability than that of the traditional on-premises PBX. A digital PBX phone system is a phone solution that connects all the desk phones in an organizations network. It is often referred to as a “VoIP phone system.” It uses the internet to connect users and callers and offers helpful features like call queuing and quality audio at a low price. PBX phone systems usually deliver business telephony features such as call forwarding, call transfer, call queue, auto-attendant, voicemail, etc. PBX systems operate by using either VoIP (Voice Over Internet Protocol) or via analog or digital phone lines. Seamless interface with the existing NEC handsets will keep immediate migration costs to a minimum.

The inconsistent use of telephones specifically across college campuses should be reviewed as the status of phones only in classrooms as typical at NC may provide emergency communication benefits not available at RCC or MVC. Engagement of key stakeholders including Safety and Emergency Planning Coordinators is encouraged with collective discussion sought to determine the pros and cons of telephones in all classrooms. The intent of meeting outcomes should be a typical operational condition to be implemented at all district campuses. District telephones should be provided at the Norco Innovation Center which currently requires on-site district staff to use cell phones for all communication as desk mount network phones are not provided.

Often overlooked benefits of maintaining traditional telephone handsets include:

- Availability of dedicated telephone handsets remove the need to search for mobile devices if not at hand.
- Hands-free communication supporting two-way communication easily achieved and supports ability for multi-tasking in an emergency while staying connected with the end-of-line communication.
- Programming of emergency call lines into the handset feature sets allows for one-touch dial-out if assistance is required.
- Reliability of communication connection via the network maintains communication capability, especially in areas where cellular coverage may be affected by built environment conditions or lack of cellular service.

Continuation of E911 Multi-Line Telephone System (MLTS) requirements in compliance with Federal Communications Commission (FCC) and California Public Utilities Commission (CPUC) regulatory directives should be maintained.²⁷ Maintaining compliance with federal²⁸, state, and local regulations is important for public safety, reduces potential district liability, and ensures that the district is engaging in emergency management and communication best practices.

Continued provision of single POTS lines at the college campuses is recommended, providing back-up and availability at dedicated Emergency Operations Center (EOCs) spaces to network and cellular communications. Scheduled verification of the landline status should be validated regularly to ensure that if needed, there is dial-

²⁷ [MLTS: E911 Requirements for Service Providers of Multi-Line Telephone Systems \(ca.gov\)](#)

²⁸ [Kari's Law and RAY BAUM's Act Oct 2020 \(911.gov\)](#)



out service supported. Providing POTS lines at the downtown Riverside facilities is non-essential with cellular service appearing strong throughout all buildings.

Mobile Applications

Findings: RCCD uses the RAVE Alert²⁹ emergency notification system, a part of a solution provided by RAVE Mobile Safety a Motorola Solutions Company. It is understood that all students and district employees are automatically enrolled in the RAVE Alert service with mass notification and/or targeted messages issued by Short Message Service (SMS) to mobile phones. The RAVE Alert notifications are the primary communications issued during an emergency event or lockdown by the district intended to reach a wide audience. Notifications are also received on other district owned devices that IT have ability to configure so that immediate notification of emergency notifications is received in classrooms and corridors etc. Notifications are received on district owned laptops, workstations, and display monitors, see Figure 85 for example of how RAVE Alert communications appear on network connected display monitors. Several locations currently have display monitors that were observed as turned off, monitors at MVC cafeteria exterior appeared out-of-order, and monitors in the CSS cafeteria space at NC were also observed as powered off. These display monitors are examples of equipment that can be used to communicate to congregated groups in addition to the SMS communication pushed out.



Figure 40 - Extron AV monitor at NC, display monitor at Henry W. and Alice Edna Coil School for the Arts



Figure 419 - Example of display monitor with no power at MVC

²⁹ [Rave Alert - FedRAMP-Authorized Mass Notification System \(ravemobilesafety.com\)](https://www.ravemobilesafety.com/)



The RAVE Alert notification system is a market leading communication tool and allows the district to reach a wide audience quickly. The district provides detailed login directions that are available on the district website³⁰ detailing how to opt-in to receive notifications from other campuses and district facilities that are not the “home” location of the employee or student. An option to select language preferences and provide updated personal detail information is available allowing subscribers to the service to actively participate, rather than simply being enrolled by the district automatically. Updating information provides ability to receive notifications through other means of communication (i.e., email).

It should be noted that several district employees were unaware of the RAVE Alert notification features and others shared that they had also opted out of receiving the notifications. Lack of awareness and proactively opting out of receiving notifications is concerning as key information distributed with good intent by the district may not be received and employees and or students may unknowingly approach or enter into areas of danger. Wider communication and education on the value and intent of the RAVE Alert notifications to the target audience should be considered.

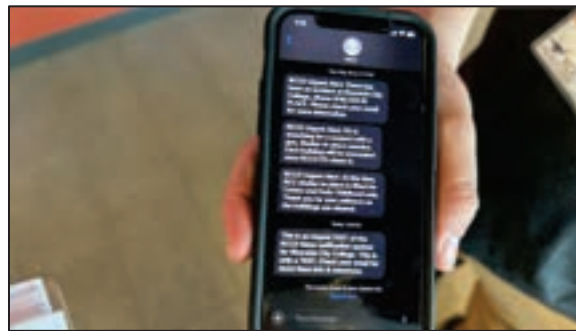


Figure 90 - Example of RAVE Alert SMS Notification on Mobile Phone

The RAVE Mobile Safety system also offers a RAVE Guardian application that is a free Smartphone-based security application that allows users to call 911, call RCCD police, set up a timed virtual escort, notify specific people about their status and location, and text RCCD Police about security threats or other problems. RAVE Guardian³¹ is an opt-in subscription application that is available for use by all currently registered RCCD students and current employees of RCCD. Subscription to the application requires the use of an RCCD email address to logon. Directions on how to download the application to smartphones are also available on the district website.

The RAVE Guardian application provides six (6) distinct features that can be used by subscribers to request help via 911, notify RCCD Police of abnormal activity, function as a safety timer for virtual escort service, create a notification tree of guardians/friends etc., serve as a tip-line with two-way communication, and provide email communication.

³⁰ [RAVE 2022.indd \(rccd.edu\)](#)

³¹ [Rave_Guardian_Trifold_GENERAL \(rccd.edu\)](#)



Recommendations: Mobile applications play an important role in today's world where technology has advanced such that many community college campus users possess ability to receive and provide text and visual coverage of activity using a cellphone. Some colleges and higher education institutions across the country, most notably the University of Colorado Boulder, have implemented removal of emergency blue phones and adopted programs where the mobile application is the core tool used for two-way communication between campus users and the university police department³².

It is recommended that the RAVE Alert notifications continue to be used by RCCD as the primary means of providing mass notification, delivering alerts through cel phones, desk phones, emails, social media, digital signage, and the district website. The RAVE Alert notifications should serve as a supplementary measure to other means of emergency and mass communication measures such as emergency phones.

It is recommended that the district continue automatically enrolling all employees and student email and cell phone data into systems as a mandatory process so that the opt-in requirements currently required by RAVE Alert are met.

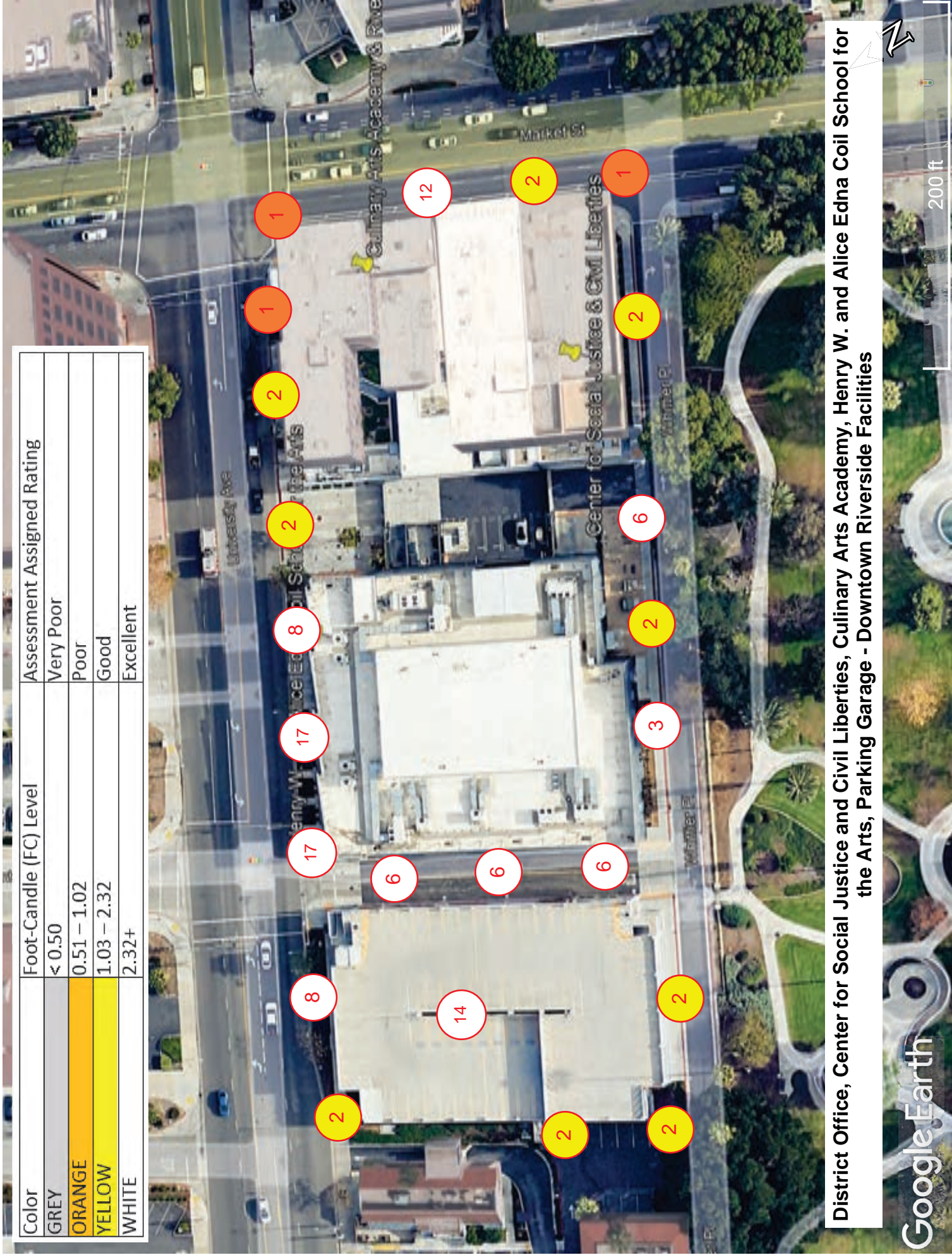
Regular testing and review of interfaced electronic displays is encouraged. Ability to provide communication to areas where campus users can visually read and or be made aware of a notification audibly should be considered, specifically using existing equipment that can enhance the safety and security program mass communication capabilities.

³² <https://www.colorado.edu/today/2015/12/14/police-chief-why-we-are-removing-campus-blue-light-phones>

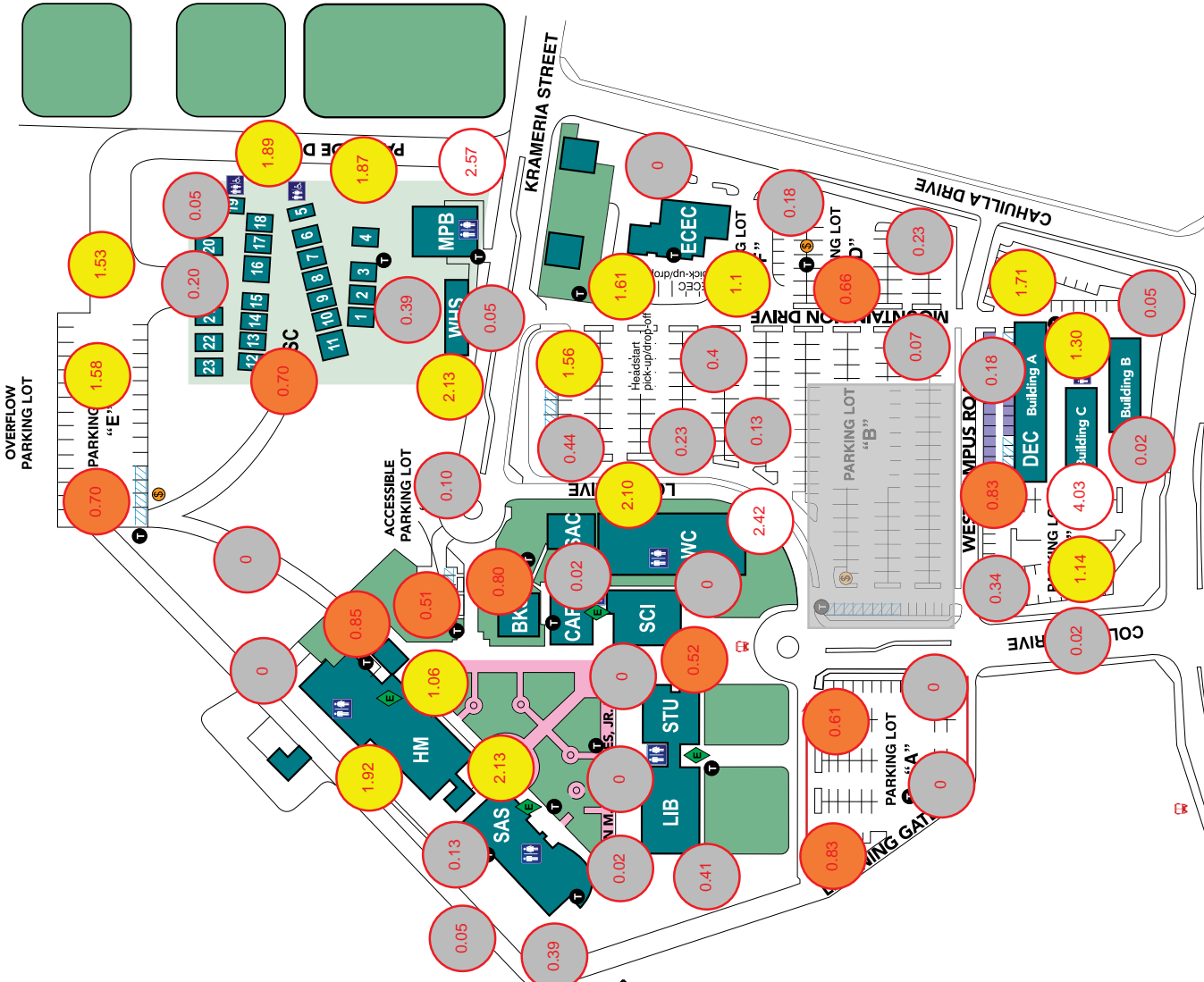


APPENDIX D – HIGH-LEVEL EXTERIOR LIGHTING ASSESSMENTS

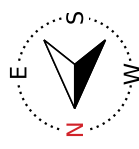
Color	Foot-Candle (FC) Level	Assessment Assigned Rating
GREY	< 0.50	Very Poor
ORANGE	0.51 – 1.02	Poor
YELLOW	1.03 – 2.32	Good
WHITE	2.32+	Excellent



District Office, Center for Social Justice and Civil Liberties, Culinary Arts Academy, Henry W. and Alice Edna Coil School for the Arts, Parking Garage - Downtown Riverside Facilities



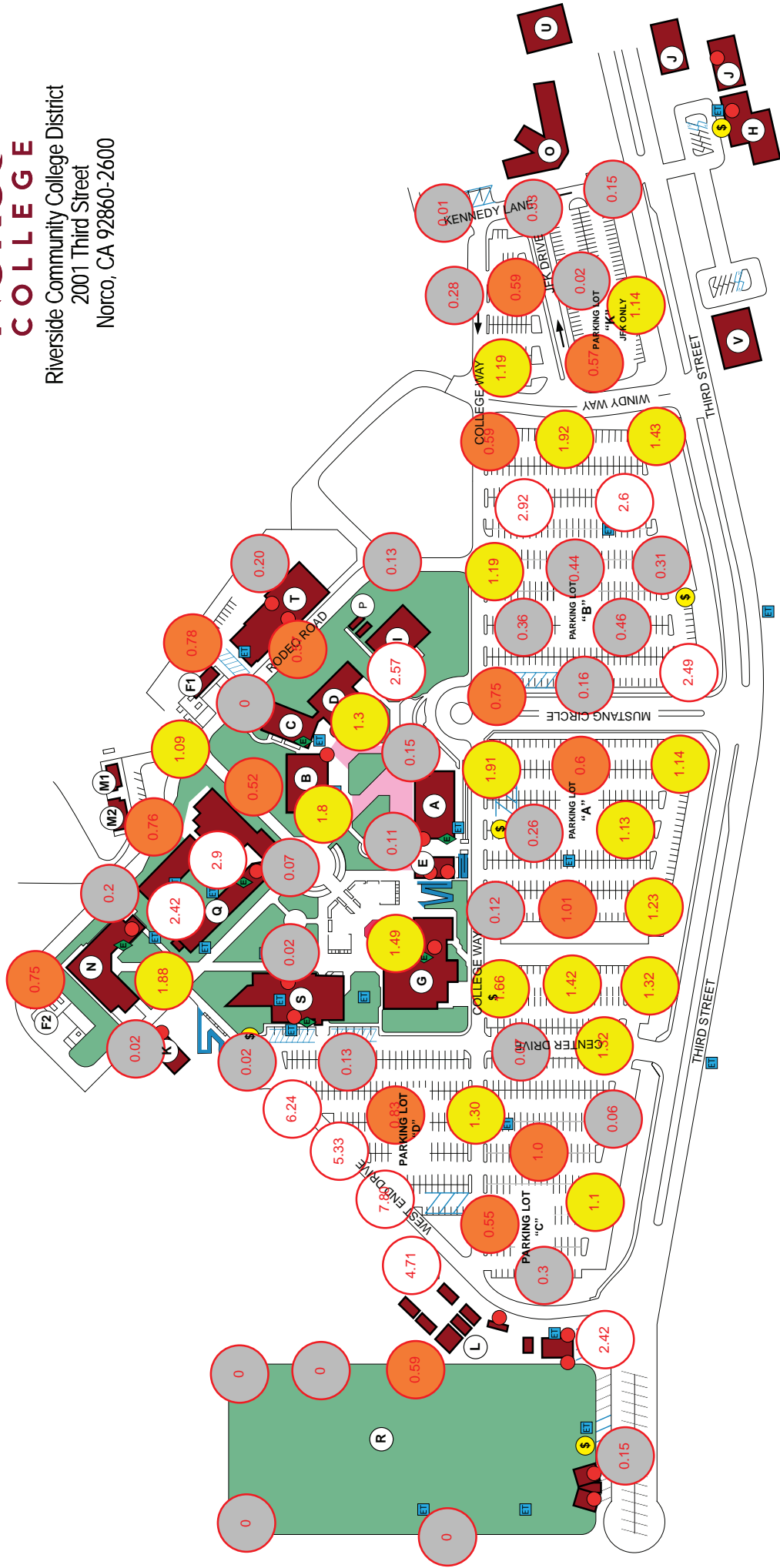
- Emergency Telephones
- Elevators
- Restrooms
- Free Speech Area
- Accessible Parking
- Patient Parking
- Parking Pay Station
- RTA Bus Stop



Color	Foot-Candle (FC) Level	Assessment Assigned Rating
GREY	< 0.50	Very Poor
ORANGE	0.51 – 1.02	Poor
YELLOW	1.03 – 2.32	Good
WHITE	2.32+	Excellent

NORCO COLLEGE

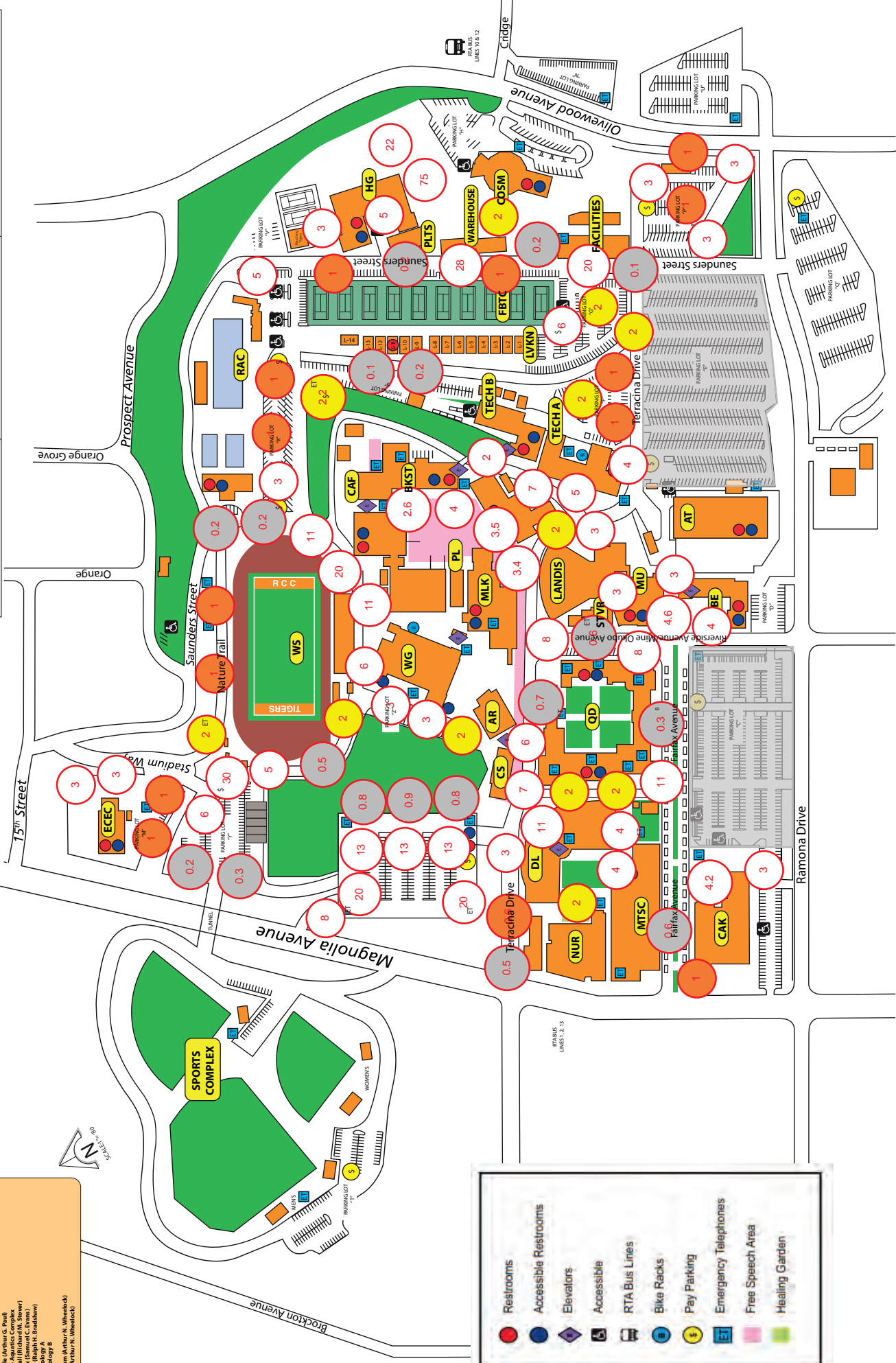
Riverside Community College District
 2001 Third Street
 Norco, CA 92860-2600



Color	Foot-Candle (FC) Level	Assessment Assigned Rating
GREY	< 0.50	Very Poor
ORANGE	0.51 - 1.02	Poor
YELLOW	1.03 - 2.32	Good
WHITE	2.32+	Excellent

Riverside City College

Color	Foot-Candle (FC) Level	Assessment Assigned Rating
GREY	< 0.50	Very Poor
ORANGE	0.51 – 1.02	Poor
YELLOW	1.03 – 2.32	Good
WHITE	2.32+	Excellent

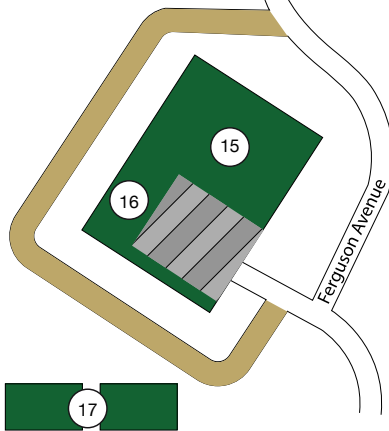
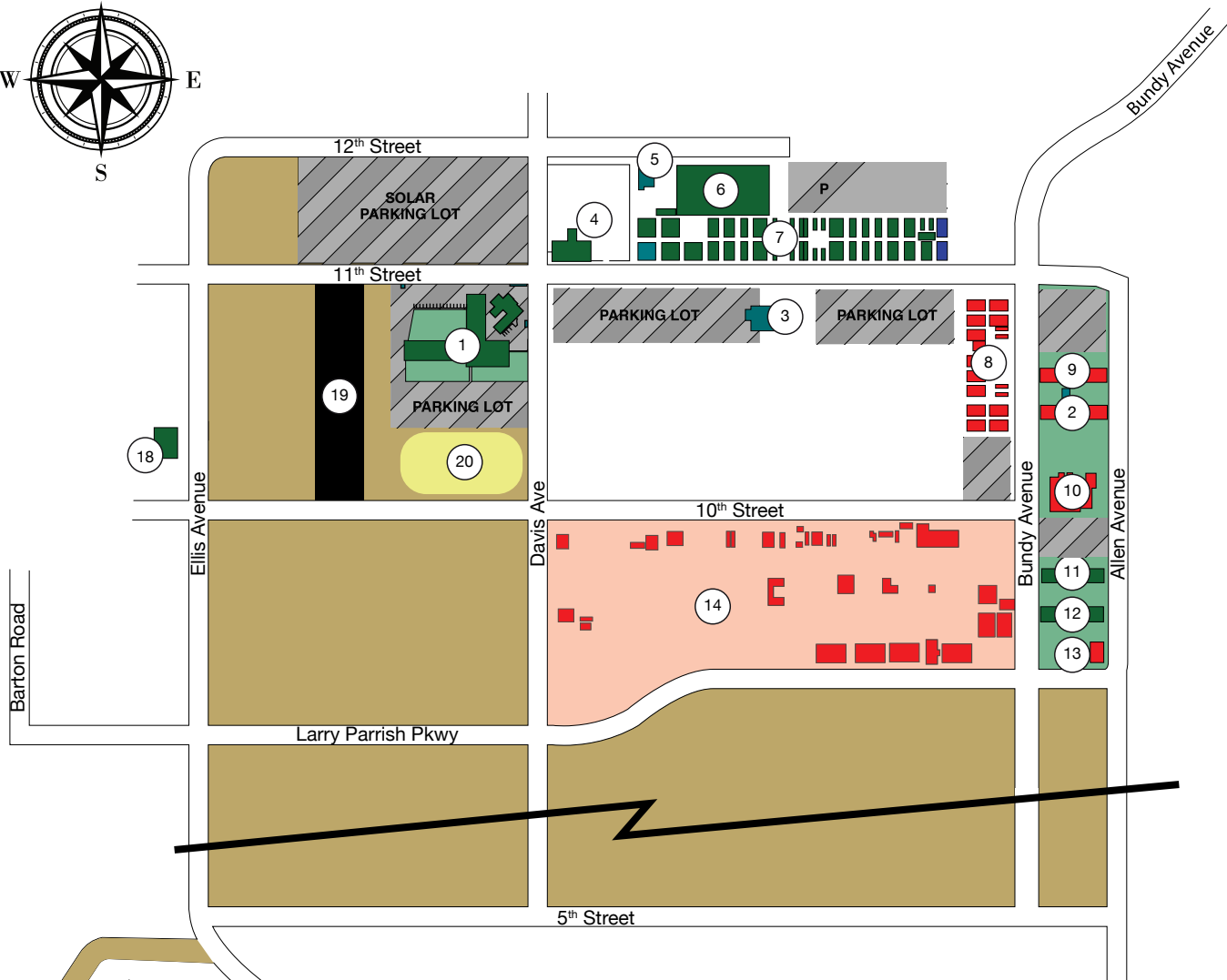
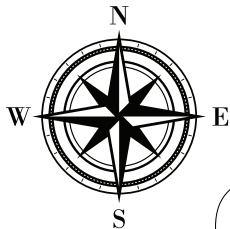


- (ART) Automotive Technology
- (BE) Business Education (Akin D. Pawel)
- (CS) Computer Services & Administration Building (Dr. Charles A. Keme)
- (CS) Ceramics
- (COSM) Cosmetology
- (D) Digital Library & Learning Resource Center (Salvador G. Rivera)
- (ECC) Early Childhood Education
- (EPFC) Fran Bushman Tennis Courts
- (H) Gymnasium (Catherine S. Hurley)
- (J) Journalism (Catherine S. Hurley)
- (L) Library (Catherine S. Hurley)
- (LW) Leukemia Center
- (LWLN) Lewin Complex
- (M) Music
- (MNR) School of Nursing
- (M) Music
- (P) Photography (Robert T. Dixon)
- (PETS) Pet Studio (Beane H. Crabree)
- (R) Radiology (Arthur C. Paul)
- (R) Radiology (Arthur C. Paul)
- (STVR) Music Hall (Richard M. Stover)
- (S) Sports Complex (Samuel C. Brown)
- (T) Technology (Arthur C. Paul)
- (TECH A) Technology A
- (TECH B) Technology B
- (T) Technology (Arthur C. Paul)
- (W) Gymnasium (Arthur N. Wheelock)
- (WS) Stadium (Arthur N. Wheelock)

- Restrooms
- Accessible Restrooms
- ◆ Elevators
- ♿ Accessible
- 🚌 RTA Bus Lines
- 🚲 Bike Racks
- 💵 Pay Parking
- ☎ Emergency Telephones
- 🗣 Free Speech Area
- 🌿 Healing Garden

Ben Clark Training Center

16791 Davis Ave., Riverside, CA 92518



- Riverside County Sheriff's Department
- California Highway Patrol
- Moreno Valley College

- Emergency Medical Services, CAL-Fire Riverside County Fire/California Department of Forestry and Fire Protection
- Parking

1. Ben Clark Administration Building
 - RSO, CHP, Sheriff's Personnel
 - Uniform Services
2. Fire Administration
3. MVC Offices/School of Public Safety
4. Sheriff's Logistics
5. Corrections Platform
6. Academy Grinder

7. Academy Buildings
 - DT Room/Cross-Fit Gym, Bldg 1-4
 - Weight Room, Bldg 6
 - Academy Bldgs 7-12
 - SWORN TACT Staff, Bldg 13
 - MODULAR/CD TACT, Bldg 14
 - AOT Staff, Bldg 23
 - Modular Bldg 24
 - R&D, Bldg 26
 - AOT Bldgs, 25, 27-35
 - CHP, Bldgs 37-38
8. Fire/EMS Modular Classrooms

9. Fire Dormitory
10. Auditorium/Dining Hall
11. Sheriff Dormitory
12. Scenario Building
13. Fire Gym
14. CAL-Fire Drill Grounds
15. Range
16. Scenario Village
17. Equestrian Area
18. Gas House
19. Low Speed EVOG
20. Running Track



APPENDIX E – CRIMECAST CAP (CRIMES AGAINST PERSONS AND PROPERTY) INDEX REPORTS



GENERATED FOR: SALAS O'BRIEN

SITE NAME: MORENO VALLEY COLLEGE

ADDRESS: 16130 LASSELLE STREET
MORENO VALLEY, CA 92551

CREATION DATE: JUNE 07, 2024

CRIMECAST® BASIC REPORT

CRIMECAST® Reports indicate the likelihood of crime and loss occurring at any address in the United States, Canada, Mexico, and the United Kingdom. Each report includes CAP Scores designating the risk of crime as well as detailed maps depicting those risks within a defined radius around each location.



2024 CAP INDEX® SCORE

MAX-6: 202



REPORT COMPONENTS

SCORING METHODOLOGY

This area indicates the scoring methodology being used. Reference the Appendix page for an explanation of the various methodologies.

CAP SCORES

The **National CAP Index® Score** indicates the overall risk of crime at the address.

The report also includes nine specific CAP Scores pertaining to **Crimes Against Persons** and **Crimes Against Property**, along with two **Supplemental Scores**.

CRIMECAST® MAP

The **Site Map** shows the **Block Group Score** for each "neighborhood" surrounding a given location. The **Site Map** helps depict the potential origin of criminal activity occurring at the location.

Every 10 years, the Census Bureau designates block groups in the United States. With the 2023 database release, the number of block groups increased from roughly 217,000 to over 239,000.

The CAP Index Scoring System assigns a numeric risk score and a corresponding risk shading to each block group.

MAX-6 SUMMARY PAGE

SITE NAME: MORENO VALLEY COLLEGE
ADDRESS: 16130 LASSELLE STREET, MORENO VALLEY, CA 92551

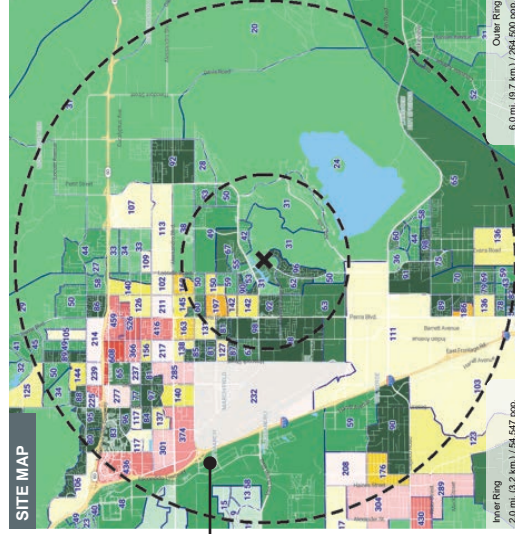
2024 NATIONAL CRIME RISK SCORES

CRIMES AGAINST PERSONS	241	CRIMES AGAINST PROPERTY	236	SUPPLEMENTAL SCORES	265
Homicide	206	Burglary	225	Simple Assault	232
Rape	218	Larceny	219	Vandalism	232
Robbery	200	Motor Vehicle Theft	419		
Aggravated Assault	264				

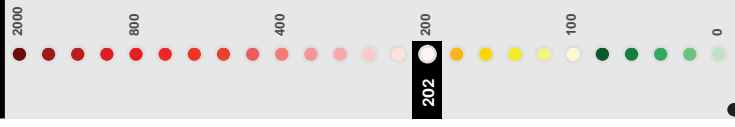
THIS SITE'S CAP INDEX® SCORE:

202

THE CRIME RISK AT THIS SITE IS 2.02 TIMES THE NATIONAL AVERAGE OF 100.



CAP SCORE SCALE



The **Heat Map** provides an alternative view of the risk of crime within the map window. CRIMECAST® Heat Maps are developed by calculating the CAP Index® Scores for every point on the map and then shading its corresponding risk level.

CAP SCORE SCALE

CAP Scores range from 0 to 2000, with 0 representing the lowest risk and 2000 the highest; 100 is average. A score of 600 is 6 times the National Average, and a score of 25 indicates a risk that is 1/4 of the National Average.

MAX-6 SUMMARY PAGE



SITE NAME: MORENO VALLEY COLLEGE
ADDRESS: 16130 LASSELLE STREET, MORENO VALLEY, CA 92551

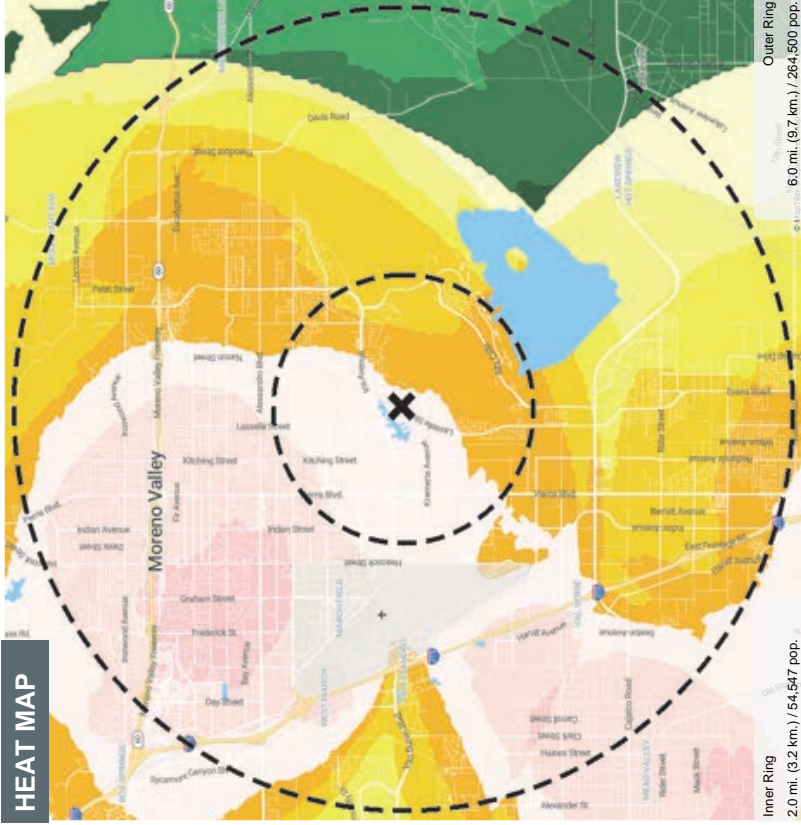
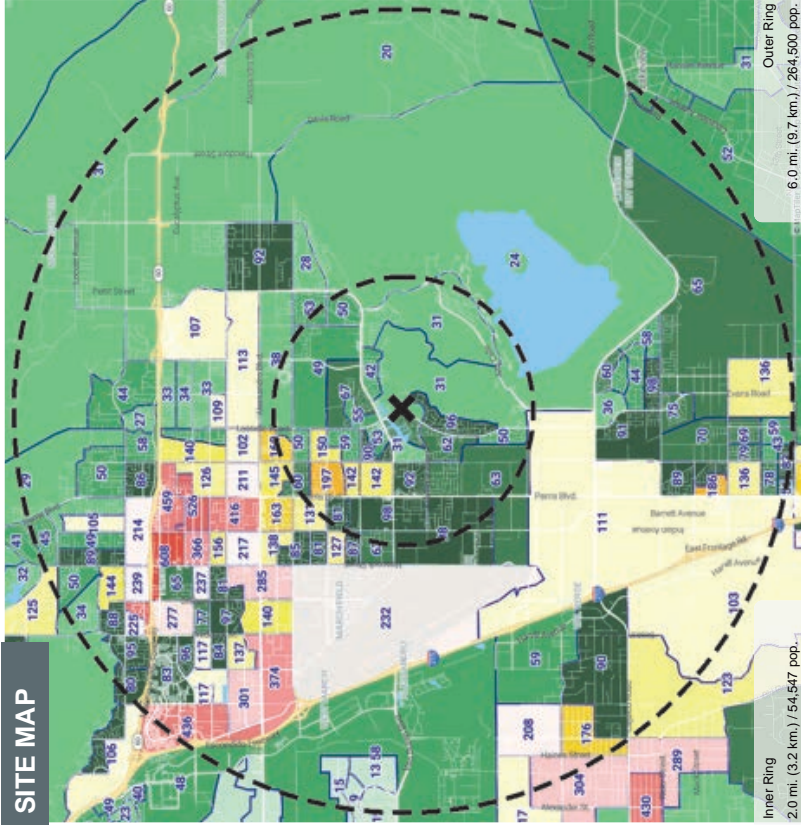
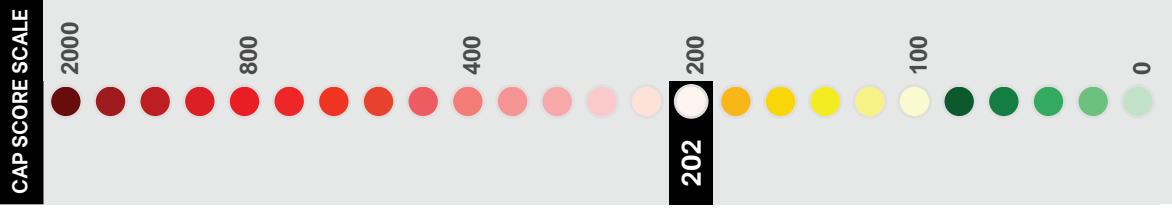
2024 NATIONAL CRIME RISK SCORES

CRIMES AGAINST PERSONS	241	CRIMES AGAINST PROPERTY	236	SUPPLEMENTAL SCORES	
Homicide	206	Burglary	225	Simple Assault	265
Rape	218	Larceny	219	Vandalism	232
Robbery	200	Motor Vehicle Theft	419		
Aggravated Assault	264				

THIS SITE'S CAP INDEX® SCORE:

202

THE CRIME RISK AT THIS SITE IS 2.02
 TIMES THE NATIONAL AVERAGE OF 100.



Creation Date: June 07, 2024
 Database Year: 2024

CRIMECAST and CAP Index are registered trademarks of CAP Index, Inc. Please note terms and conditions as presented on <https://capindex.com/terms-conditions>. ©2024 CAP Index, Inc. All rights reserved.

MAX-6 SITE MAP



SITE NAME: MORENO VALLEY COLLEGE
ADDRESS: 16130 LASSELLE STREET, MORENO VALLEY, CA 92551

2024 NATIONAL CRIME RISK SCORES

THIS SITE'S CAP INDEX® SCORE:

202

THE CRIME RISK AT THIS SITE IS 2.02
 TIMES THE NATIONAL AVERAGE OF 100.

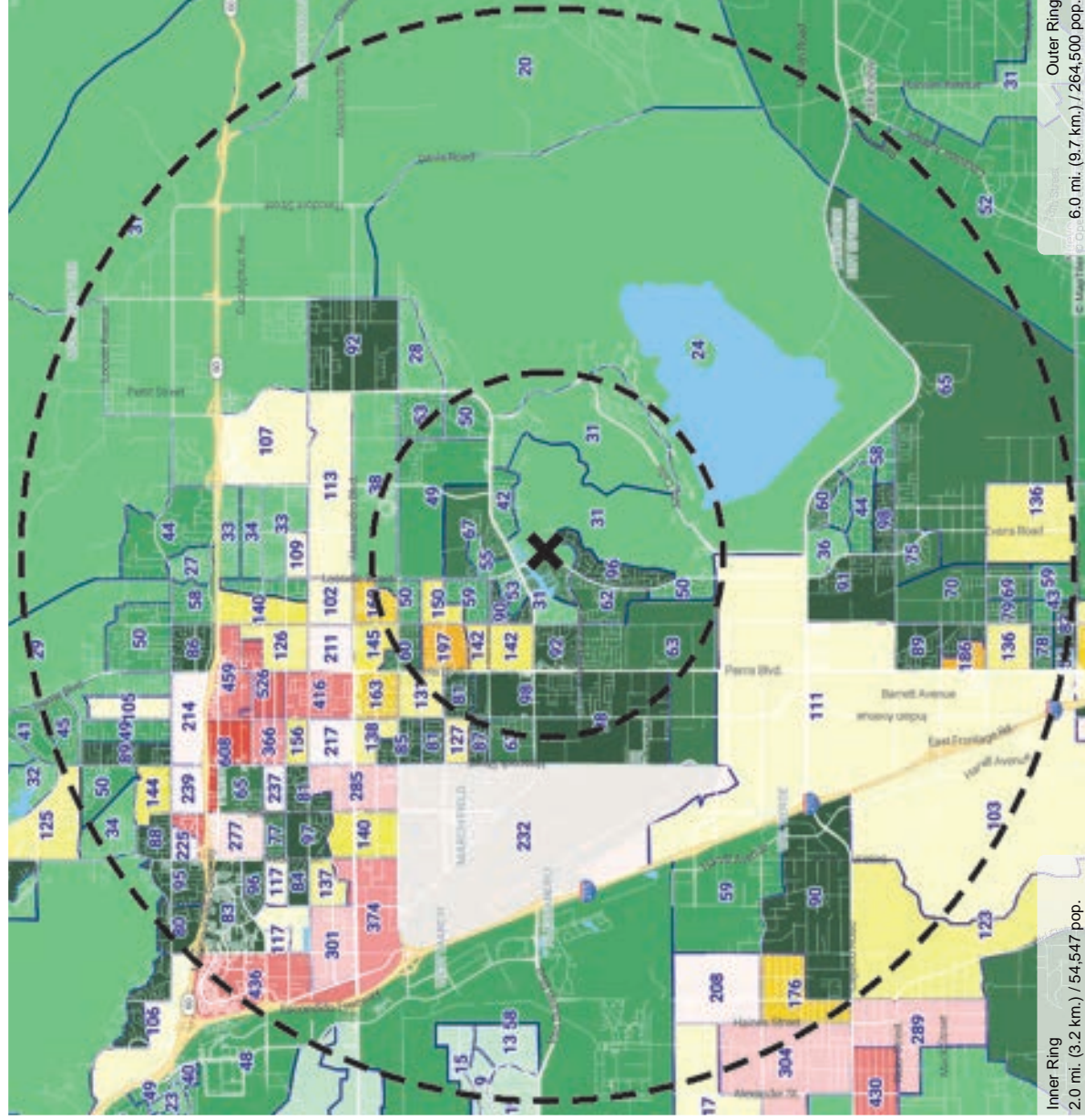
CRIMES AGAINST PERSONS 241

Homicide	206
Rape	218
Robbery	200
Aggravated Assault	264

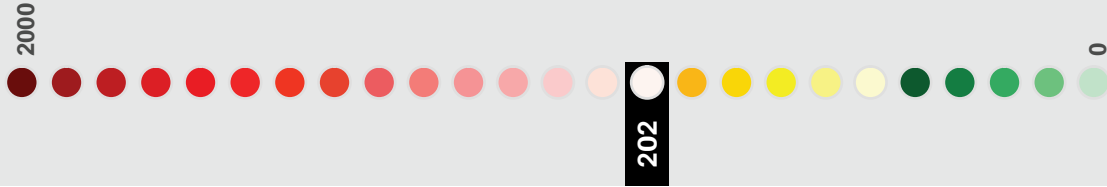
Larceny 219

SUPPLEMENTAL SCORES

Simple Assault	265
Vandalism	232



CAP SCORE SCALE



Creation Date: June 07, 2024
 Database Year: 2024

CRIMECAST and CAP Index are registered trademarks of CAP Index, Inc. Please note terms and conditions as presented on <https://capindex.com/terms-conditions>. ©2024 CAP Index, Inc. All rights reserved.

MAX-6 HEAT MAP



SITE NAME: MORENO VALLEY COLLEGE
ADDRESS: 16130 LASSELLE STREET, MORENO VALLEY, CA 92551

2024 NATIONAL CRIME RISK SCORES

THIS SITE'S CAP INDEX® SCORE:

202

THE CRIME RISK AT THIS SITE IS 2.02 TIMES THE NATIONAL AVERAGE OF 100.

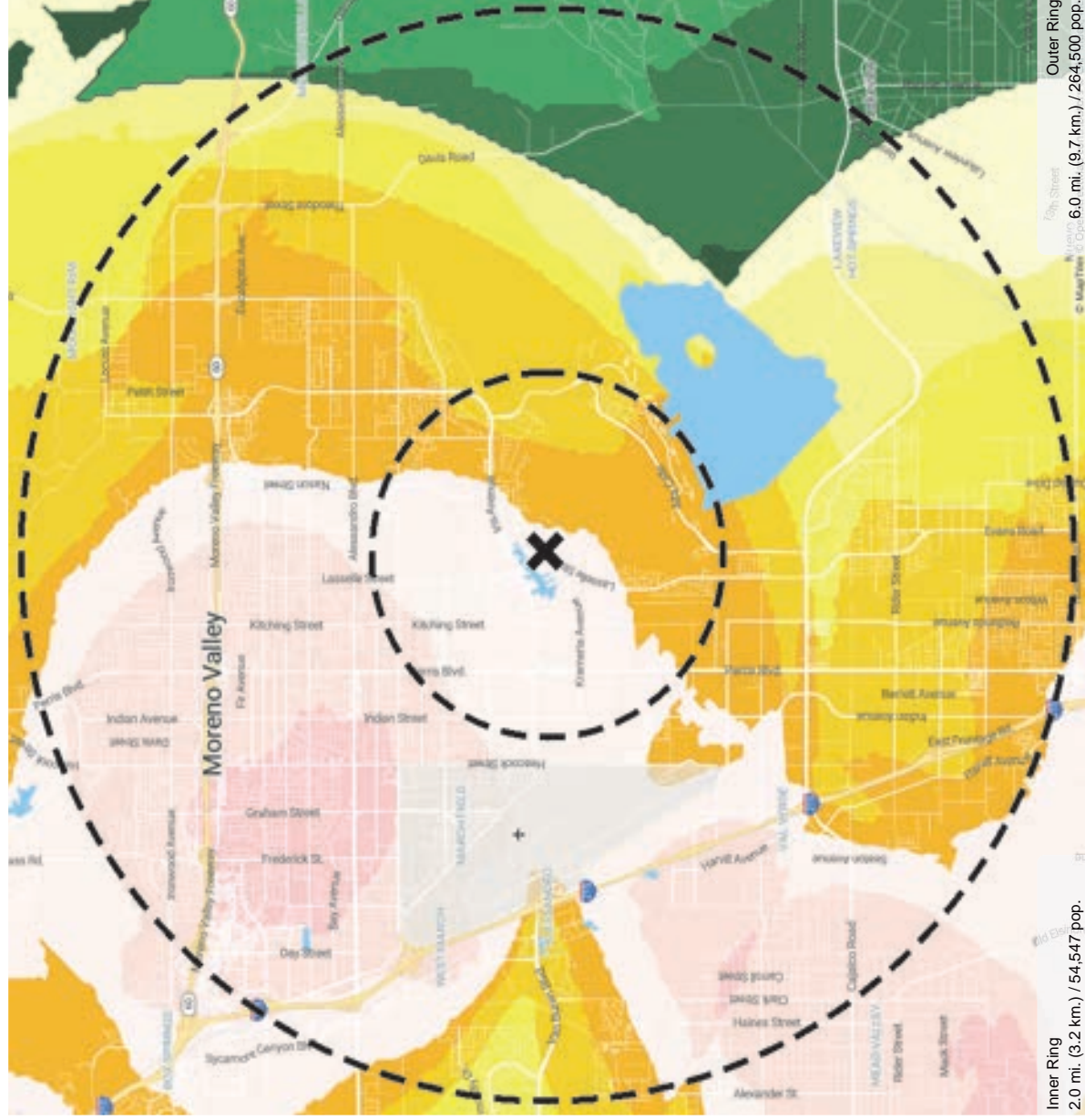
CRIMES AGAINST PERSONS 241

Homicide	206
Rape	218
Robbery	200
Aggravated Assault	264

Larceny 219

SUPPLEMENTAL SCORES

Simple Assault	265
Vandalism	232



Creation Date: June 07, 2024
 Database Year: 2024

CRIMECAST and CAP Index are registered trademarks of CAP Index, Inc. Please note terms and conditions as presented on <https://capindex.com/terms-conditions>. ©2024 CAP Index, Inc. All rights reserved.

MAX-6 SCORE SUMMARY



SITE NAME: MORENO VALLEY COLLEGE
ADDRESS: 16130 LASSELLE STREET, MORENO VALLEY, CA 92551

The Score Summary includes a total of 108 risk scores - 12 for each of 3 geographic levels and 3 time periods. 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 State Scores compare the site to the state averages and the County Scores to the county averages. Past, Current, and Projected risk scores are provided to allow for trending.

GEOGRAPHIC LEVEL	UNITED STATES			CALIFORNIA			RIVERSIDE COUNTY		
	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029
CRIME RISK SCORES									
CAP Index® Score	195	202	194	164	168	164	184	185	183
CRIMES AGAINST PERSONS	232	241	228	201	209	202	191	193	188
Homicide	202	206	200	226	229	225	195	200	203
Rape	215	218	211	222	227	225	183	178	179
Robbery	205	200	193	164	158	154	198	188	186
Aggravated Assault	256	264	248	226	234	226	196	196	191
CRIMES AGAINST PROPERTY	243	236	217	208	204	194	230	228	216
Burglary	239	225	189	211	196	169	218	220	193
Larceny	218	219	207	208	211	206	235	236	228
Motor Vehicle Theft	432	419	377	230	228	216	253	253	238
SUPPLEMENTAL SCORES									
Simple Assault	259	265	258	287	296	295	230	226	226
Vandalism	243	232	225	271	265	265	243	233	233



ABOUT CRIMECAST SCORING

THE CAP INDEX® SCORING SYSTEM

The CAP Index® Scoring System uses sophisticated forecasting techniques that combine demographic and business statistics with crime and loss data to calculate crime risk. The foundation of our forecasting approach is the “Social Disorganization Theory,” which asserts that higher degrees of social discord in a neighborhood tend to correlate with higher levels of crime.



SCORING METHODOLOGIES

CAP Scores for a specific business application are generated using one of four CAP Index® Scoring Methodologies. These scoring methodologies account for the fact that perpetrators often travel varying distances to commit crimes (the “journey to crime”) depending on the target. The scoring methodologies also consider the nature and attractiveness of different types of targets for different types of crimes. Each methodology designates a progressively larger “sphere of influence” that is used to assess the risk of crime. Each sphere is defined by a maximum geographic radius or a population threshold. These spheres have different components that drive the overall crime risk score. The inner part of the sphere focuses on the nearest neighborhoods and receives the higher percentage of the weight. The outer part of the sphere considers more distant avenues of vulnerability and receives the remaining percentage of the weight.

Scoring Methodology	Outer Ring / Population for Assessment	Weight	Inner Ring / Population for Assessment	Weight
MAX-1	1 mile (1.6 km.) or 25,000 people	N/A	1 mile (1.6 km.) or 25,000 people	100%
MAX-3	3 miles (4.8 km.) or 100,000 people	20%	1 mile (1.6 km.) or 25,000 people	80%
MAX-6	6 miles (9.7 km.) or 400,000 people	20%	2 miles (3.2 km.) or 100,000 people	80%
MAX-12	12 miles (19.3 km.) or 1,600,000 people	33%	4 miles (6.4 km.) or 400,000 people	67%

CAP SCORE SCALE

CAP Scores range from 0 to 2000, with 0 representing the lowest risk and 2000 the highest; 100 is average. A score of 600 is 6 times the National Average, and a score of 25 indicates a risk that is 1/4 of the National Average.



RELIED UPON
BY OVER
80%
OF THE
FORTUNE 100

THE LEADERS IN CRIME RISK FORECASTING

CAP Index empowers organizations to make better-informed decisions throughout the security planning and security management cycle. Whether you are opening a new location, planning security measures for your existing locations, or conducting services off-site, our validated crime risk intelligence will help you create impactful security solutions to protect your customers, employees, assets, and your bottom line.



CRIMECAST® DATA & REPORTS

Quantify and visualize your risk with our detailed, industry-leading, site-specific crime risk reports.



RISK CONSULTING & ANALYTICS

Elevate your security program by having our team of consultants produce a crime risk scoring system tailored to your organization's needs.



TECHNOLOGY, PLATFORMS & MODULES

Manage your security planning process and loss prevention program from one dashboard.

HOW WE HELP: ASSESS YOUR RISK AND OUTSMART CRIME®



Make your customers, employees, and assets safer



Reduce crime, loss, and claims



Optimize the return from your security investment



Ensure compliance with industry standards



Reduce litigation and avoid adverse judgments



Protect your brand

800.227.7475 | 001.610.903.3000 | capindex.com | askcap@capindex.com



GENERATED FOR: SALAS O'BRIEN

SITE NAME: NORCO COLLEGE

ADDRESS: 2001 3RD STREET
NORCO, CA 92860

CREATION DATE: JUNE 07, 2024

CRIMECAST® BASIC REPORT

CRIMECAST® Reports indicate the likelihood of crime and loss occurring at any address in the United States, Canada, Mexico, and the United Kingdom. Each report includes CAP Scores designating the risk of crime as well as detailed maps depicting those risks within a defined radius around each location.



2024 CAP INDEX® SCORE

MAX-3: 261



REPORT COMPONENTS

SCORING METHODOLOGY

This area indicates the scoring methodology being used. Reference the Appendix page for an explanation of the various methodologies.

CAP SCORES

The **National CAP Index® Score** indicates the overall risk of crime at the address.

The report also includes nine specific CAP Scores pertaining to **Crimes Against Persons** and **Crimes Against Property**, along with two **Supplemental Scores**.

CRIMECAST® MAP

The **Site Map** shows the **Block Group Score** for each "neighborhood" surrounding a given location. The **Site Map** helps depict the potential origin of criminal activity occurring at the location.

Every 10 years, the Census Bureau designates block groups in the United States. With the 2023 database release, the number of block groups increased from roughly 217,000 to over 239,000.

The CAP Index Scoring System assigns a numeric risk score and a corresponding risk shading to each block group.

MAX-3 SUMMARY PAGE

SITE NAME: NORCO COLLEGE
ADDRESS: 2001 3RD STREET, NORCO, CA 92860

2024 NATIONAL CRIME RISK SCORES

CRIMES AGAINST PERSONS	437	CRIMES AGAINST PROPERTY	295	SUPPLEMENTAL SCORES	418
Homicide	408	Burglary	274	Simple Assault	317
Rape	262	Larceny	276	Vandalism	317
Robbery	258	Motor Vehicle Theft	440		
Aggravated Assault	562				

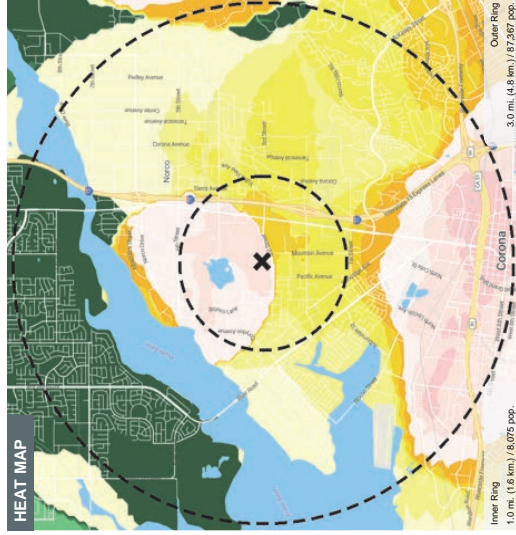
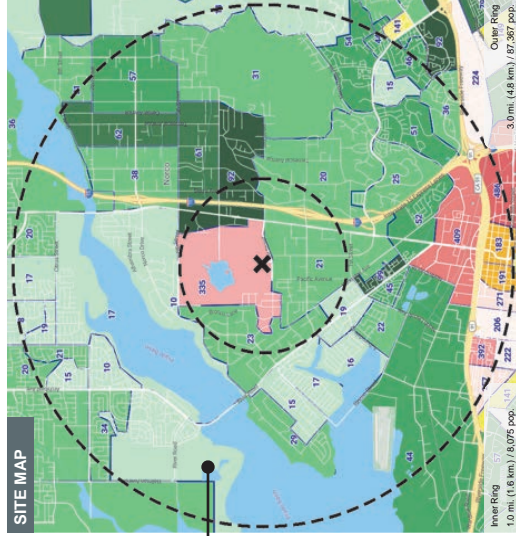
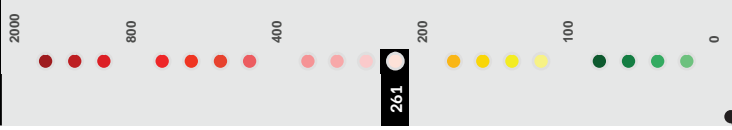
THIS SITE'S CAP INDEX® SCORE:

261

THE CRIME RISK AT THIS SITE IS 2.61 TIMES THE NATIONAL AVERAGE OF 100.



CAP SCORE SCALE



The **Heat Map** provides an alternative view of the risk of crime within the map window. CRIMECAST® Heat Maps are developed by calculating the CAP Index® Scores for every point on the map and then shading its corresponding risk level.

CAP SCORE SCALE

CAP Scores range from 0 to 2000, with 0 representing the lowest risk and 2000 the highest; 100 is average. A score of 600 is 6 times the National Average, and a score of 25 indicates a risk that is 1/4 of the National Average.

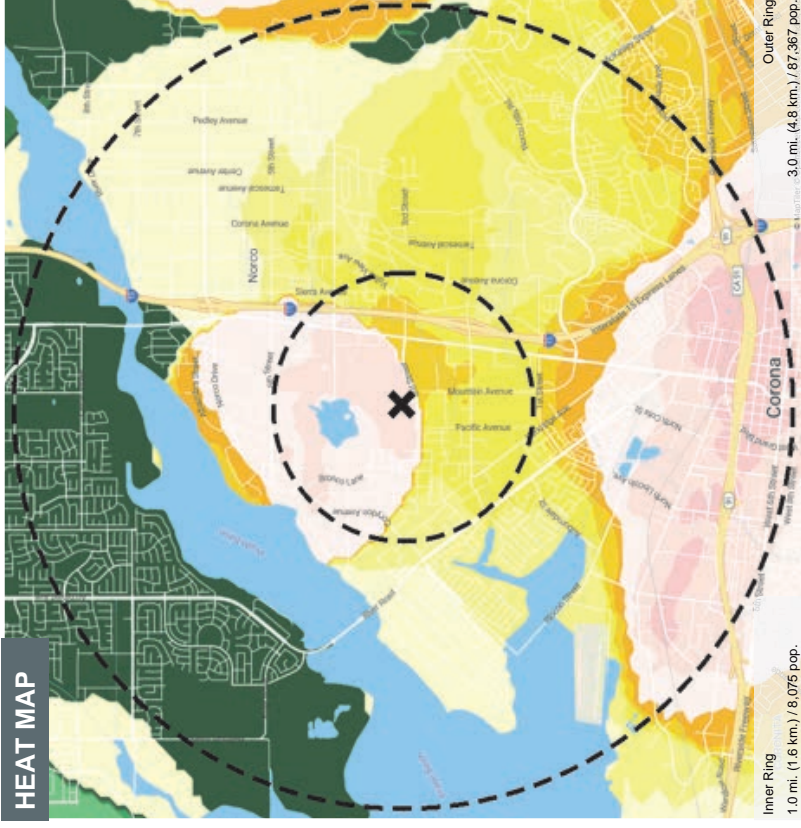
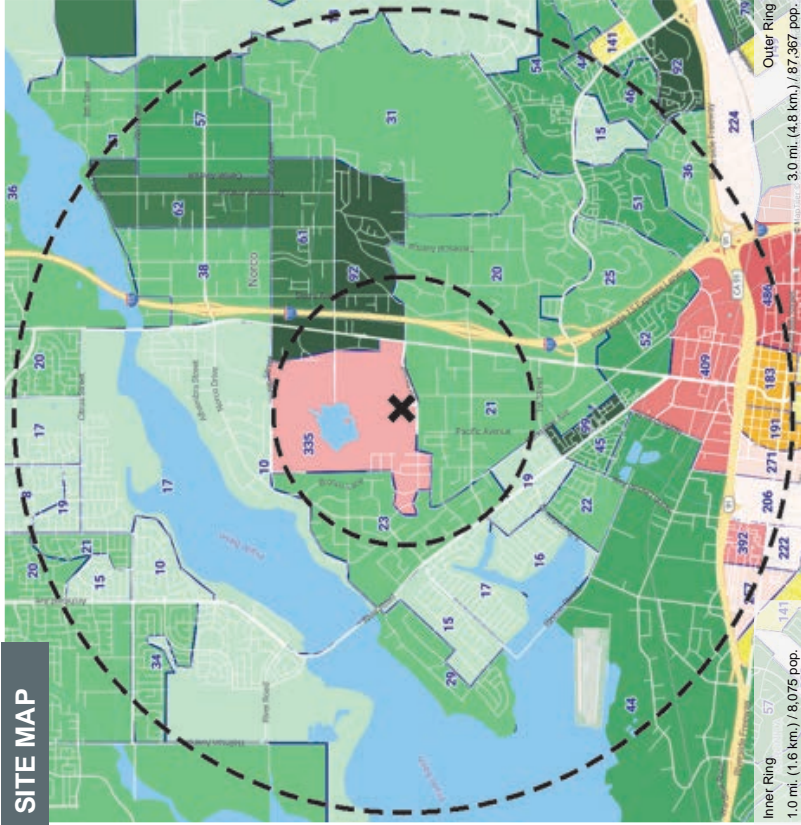
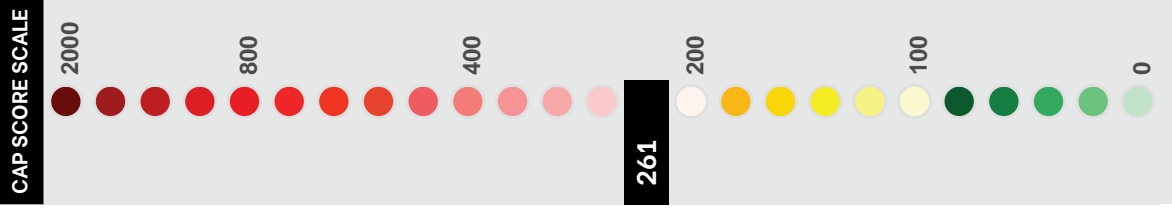
SITE NAME: NORCO COLLEGE

ADDRESS: 2001 3RD STREET, NORCO, CA 92860

2024 NATIONAL CRIME RISK SCORES

THIS SITE'S CAP INDEX® SCORE:	437		295			
	CRIMES AGAINST PERSONS	CRIMES AGAINST PROPERTY	SUPPLEMENTAL SCORES			
261	Homicide	408	Burglary	274	Simple Assault	418
	Rape	262	Larceny	276	Vandalism	317
	Robbery	258	Motor Vehicle Theft	440		
	Aggravated Assault	562				

THE CRIME RISK AT THIS SITE IS 2.61
TIMES THE NATIONAL AVERAGE OF 100.



MAX - 3 SITE MAP



SITE NAME: NORCO COLLEGE
ADDRESS: 2001 3RD STREET, NORCO, CA 92860

2024 NATIONAL CRIME RISK SCORES

THIS SITE'S CAP INDEX® SCORE:

261

THE CRIME RISK AT THIS SITE IS 2.61
 TIMES THE NATIONAL AVERAGE OF 100.

CRIMES AGAINST PERSONS 437

Homicide	408
Rape	262

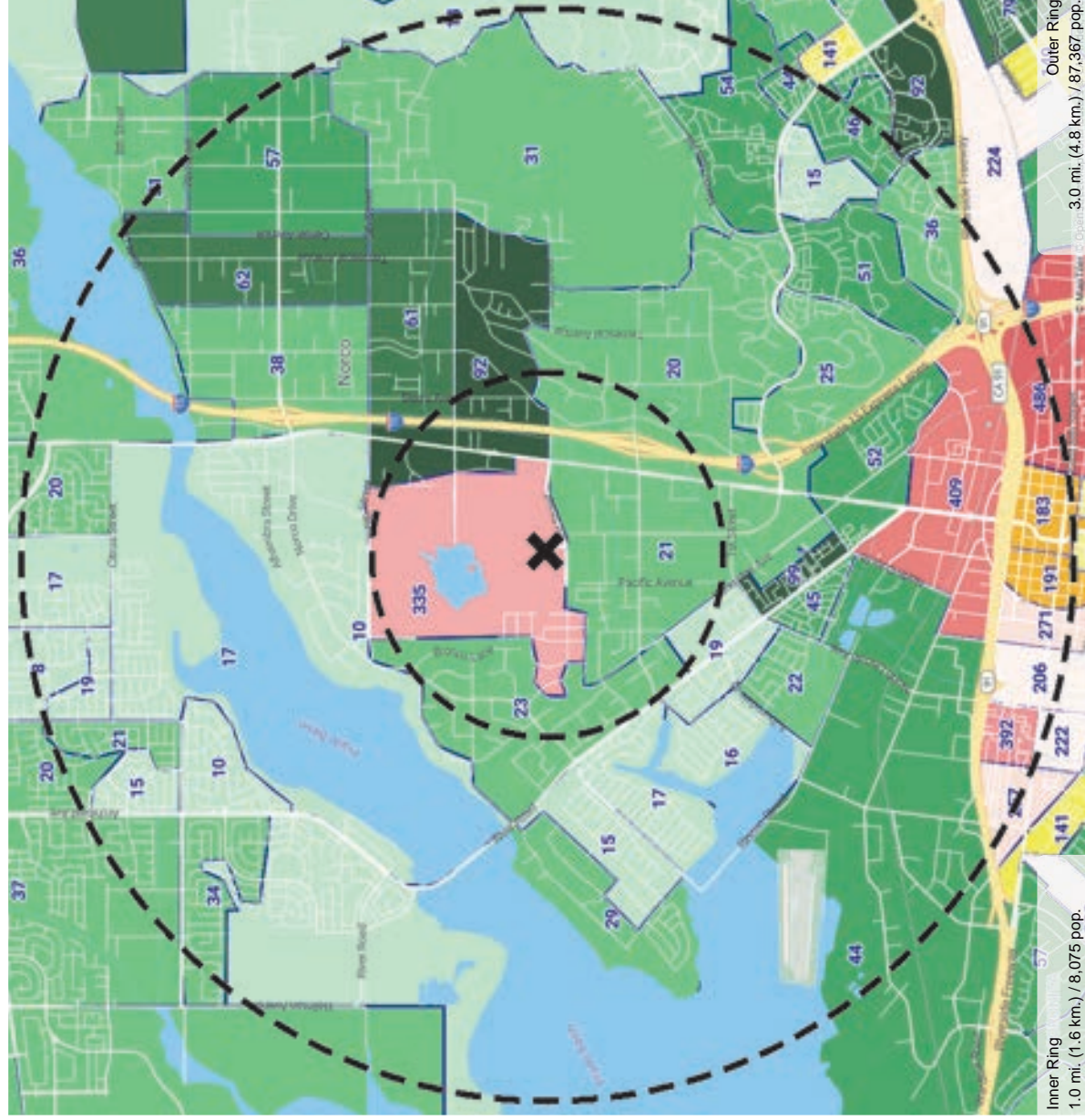
Aggravated Assault 562

CRIMES AGAINST PROPERTY 295

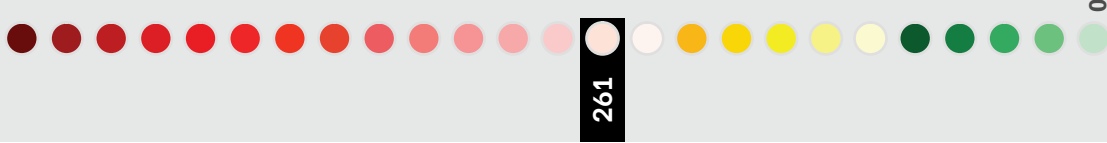
Burglary	274
Larceny	276

SUPPLEMENTAL SCORES

Simple Assault	418
Vandalism	317



CAP SCORE SCALE



Creation Date: June 07, 2024
 Database Year: 2024

CRIMECAST and CAP Index are registered trademarks of CAP Index, Inc. Please note terms and conditions as presented on <https://capindex.com/terms-conditions>. ©2024 CAP Index, Inc. All rights reserved.

MAX-3 HEAT MAP



SITE NAME: NORCO COLLEGE
ADDRESS: 2001 3RD STREET, NORCO, CA 92860

2024 NATIONAL CRIME RISK SCORES

THIS SITE'S CAP INDEX® SCORE:

261

THE CRIME RISK AT THIS SITE IS 2.61
 TIMES THE NATIONAL AVERAGE OF 100.

CRIMES AGAINST PERSONS 437

Homicide	408
Rape	262

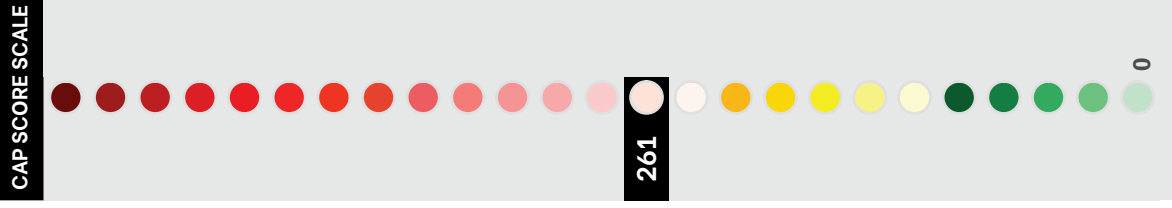
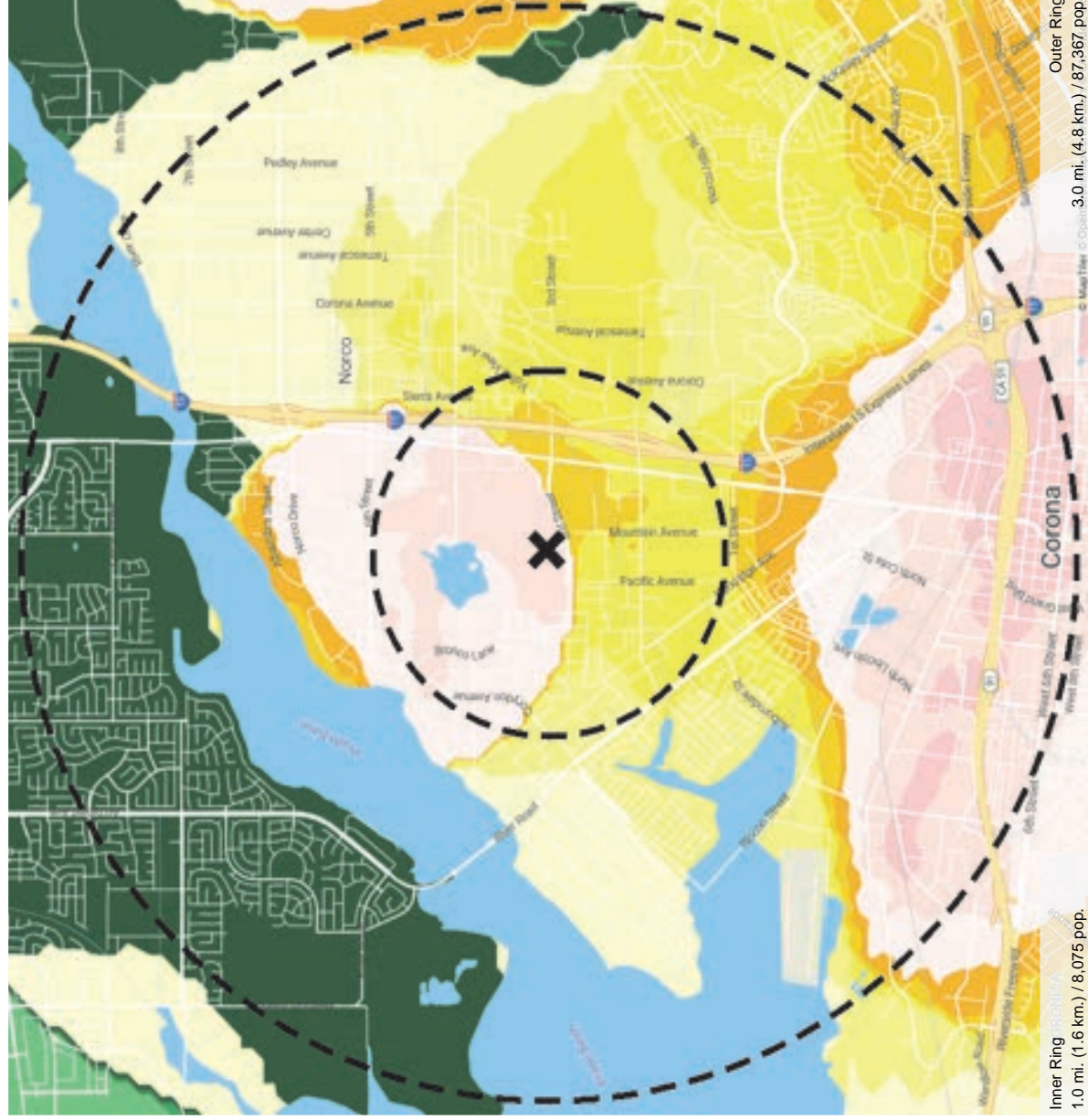
Aggravated Assault 562

CRIMES AGAINST PROPERTY 295

Burglary	274
Larceny	276

SUPPLEMENTAL SCORES

Simple Assault	418
Vandalism	317



Creation Date: June 07, 2024
 Database Year: 2024

CRIMECAST and CAP Index are registered trademarks of CAP Index, Inc. Please note terms and conditions as presented on <https://capindex.com/terms-conditions>. ©2024 CAP Index, Inc. All rights reserved.

MAX -3 SCORE SUMMARY



SITE NAME: NORCO COLLEGE
ADDRESS: 2001 3RD STREET, NORCO, CA 92860

The Score Summary includes a total of 108 risk scores - 12 for each of 3 geographic levels and 3 time periods. 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 State Scores compare the site to the state averages and the County Scores to the county averages. Past, Current, and Projected risk scores are provided to allow for trending.

GEOGRAPHIC LEVEL	UNITED STATES			CALIFORNIA			RIVERSIDE COUNTY		
	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029
CRIME RISK SCORES									
CAP Index® Score	265	261	259	223	217	219	250	239	244
CRIMES AGAINST PERSONS	450	437	423	390	378	375	371	349	349
Homicide	449	408	418	502	454	471	434	396	424
Rape	229	262	250	237	273	267	195	214	212
Robbery	270	258	259	216	203	207	261	243	250
Aggravated Assault	581	562	541	512	498	494	445	417	416
CRIMES AGAINST PROPERTY	367	295	282	315	255	253	347	285	281
Burglary	359	274	271	317	239	243	328	267	277
Larceny	338	276	260	322	266	259	364	297	286
Motor Vehicle Theft	541	440	423	288	239	242	316	265	267
SUPPLEMENTAL SCORES									
Simple Assault	409	418	401	453	466	458	363	357	351
Vandalism	325	317	305	363	362	360	325	319	315



ABOUT CRIMECAST SCORING

THE CAP INDEX® SCORING SYSTEM

The CAP Index® Scoring System uses sophisticated forecasting techniques that combine demographic and business statistics with crime and loss data to calculate crime risk. The foundation of our forecasting approach is the “Social Disorganization Theory,” which asserts that higher degrees of social discord in a neighborhood tend to correlate with higher levels of crime.



SCORING METHODOLOGIES

CAP Scores for a specific business application are generated using one of four CAP Index® Scoring Methodologies. These scoring methodologies account for the fact that perpetrators often travel varying distances to commit crimes (the “journey to crime”) depending on the target. The scoring methodologies also consider the nature and attractiveness of different types of targets for different types of crimes. Each methodology designates a progressively larger “sphere of influence” that is used to assess the risk of crime. Each sphere is defined by a maximum geographic radius or a population threshold. These spheres have different components that drive the overall crime risk score. The inner part of the sphere focuses on the nearest neighborhoods and receives the higher percentage of the weight. The outer part of the sphere considers more distant avenues of vulnerability and receives the remaining percentage of the weight.

Scoring Methodology	Outer Ring / Population for Assessment	Weight	Inner Ring / Population for Assessment	Weight
MAX-1	1 mile (1.6 km.) or 25,000 people	N/A	1 mile (1.6 km.) or 25,000 people	100%
MAX-3	3 miles (4.8 km.) or 100,000 people	20%	1 mile (1.6 km.) or 25,000 people	80%
MAX-6	6 miles (9.7 km.) or 400,000 people	20%	2 miles (3.2 km.) or 100,000 people	80%
MAX-12	12 miles (19.3 km.) or 1,600,000 people	33%	4 miles (6.4 km.) or 400,000 people	67%

CAP SCORE SCALE

CAP Scores range from 0 to 2000, with 0 representing the lowest risk and 2000 the highest; 100 is average. A score of 600 is 6 times the National Average, and a score of 25 indicates a risk that is 1/4 of the National Average.



RELIED UPON
BY OVER
80%
OF THE
FORTUNE 100

THE LEADERS IN CRIME RISK FORECASTING

CAP Index empowers organizations to make better-informed decisions throughout the security planning and security management cycle. Whether you are opening a new location, planning security measures for your existing locations, or conducting services off-site, our validated crime risk intelligence will help you create impactful security solutions to protect your customers, employees, assets, and your bottom line.



CRIMECAST® DATA & REPORTS

Quantify and visualize your risk with our detailed, industry-leading, site-specific crime risk reports.



RISK CONSULTING & ANALYTICS

Elevate your security program by having our team of consultants produce a crime risk scoring system tailored to your organization's needs.



TECHNOLOGY, PLATFORMS & MODULES

Manage your security planning process and loss prevention program from one dashboard.

HOW WE HELP: ASSESS YOUR RISK AND OUTSMART CRIME®



Make your customers, employees, and assets safer



Reduce crime, loss, and claims



Optimize the return from your security investment



Ensure compliance with industry standards



Reduce litigation and avoid adverse judgments



Protect your brand

800.227.7475 | 001.610.903.3000 | capindex.com | askcap@capindex.com



GENERATED FOR: SALAS O'BRIEN

SITE NAME: RIVERSIDE COMMUNITY COLLEGE

ADDRESS: 4800 MAGNOLIA AVENUE
RIVERSIDE, CA 92506

CREATION DATE: JUNE 07, 2024

CRIMECAST® BASIC REPORT

CRIMECAST® Reports indicate the likelihood of crime and loss occurring at any address in the United States, Canada, Mexico, and the United Kingdom. Each report includes CAP Scores designating the risk of crime as well as detailed maps depicting those risks within a defined radius around each location.



2024 CAP INDEX® SCORE

MAX-3: 229



REPORT COMPONENTS

SCORING METHODOLOGY

This area indicates the scoring methodology being used. Reference the Appendix page for an explanation of the various methodologies.

CAP SCORES

The **National CAP Index® Score** indicates the overall risk of crime at the address.

The report also includes nine specific CAP Scores pertaining to **Crimes Against Persons** and **Crimes Against Property**, along with two **Supplemental Scores**.

CRIMECAST® MAP

The **Site Map** shows the **Block Group Score** for each "neighborhood" surrounding a given location. The **Site Map** helps depict the potential origin of criminal activity occurring at the location.

Every 10 years, the Census Bureau designates block groups in the United States. With the 2023 database release, the number of block groups increased from roughly 217,000 to over 239,000.

The CAP Index Scoring System assigns a numeric risk score and a corresponding risk shading to each block group.

MAX - 3 SUMMARY PAGE

SITE NAME: RIVERSIDE COMMUNITY COLLEGE
ADDRESS: 4800 MAGNOLIA AVENUE, RIVERSIDE, CA 92506

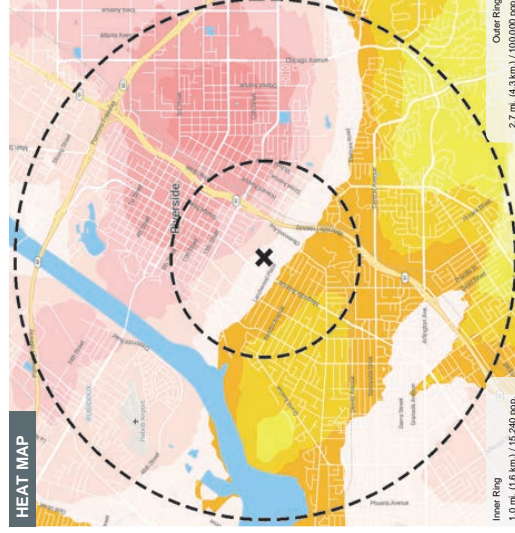
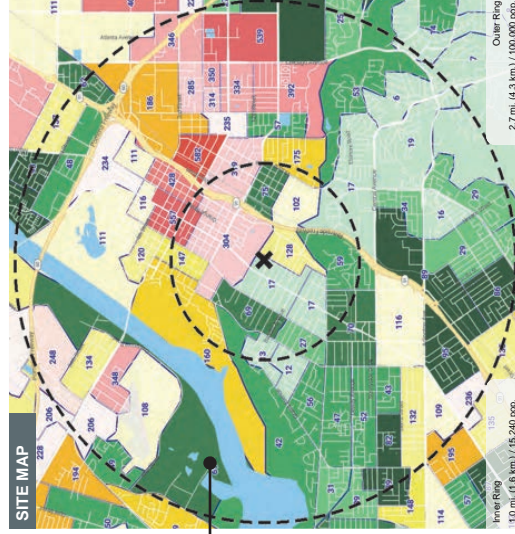
2024 NATIONAL CRIME RISK SCORES

CRIMES AGAINST PERSONS	257	CRIMES AGAINST PROPERTY	300	SUPPLEMENTAL SCORES	
Homicide	184	Burglary	408	Simple Assault	233
Rape	231	Larceny	357	Vandalism	294
Robbery	249	Motor Vehicle Theft	460		
Aggravated Assault	275				

THIS SITE'S CAP INDEX® SCORE:

229

THE CRIME RISK AT THIS SITE IS 2.29 TIMES THE NATIONAL AVERAGE OF 100.



The **Heat Map** provides an alternative view of the risk of crime within the map window. CRIMECAST® Heat Maps are developed by calculating the CAP Index® Scores for every point on the map and then shading its corresponding risk level.

CAP SCORE SCALE

CAP Scores range from 0 to 2000, with 0 representing the lowest risk and 2000 the highest; 100 is average. A score of 600 is 6 times the National Average, and a score of 25 indicates a risk that is 1/4 of the National Average.

SITE NAME: RIVERSIDE COMMUNITY COLLEGE
ADDRESS: 4800 MAGNOLIA AVENUE, RIVERSIDE, CA 92506

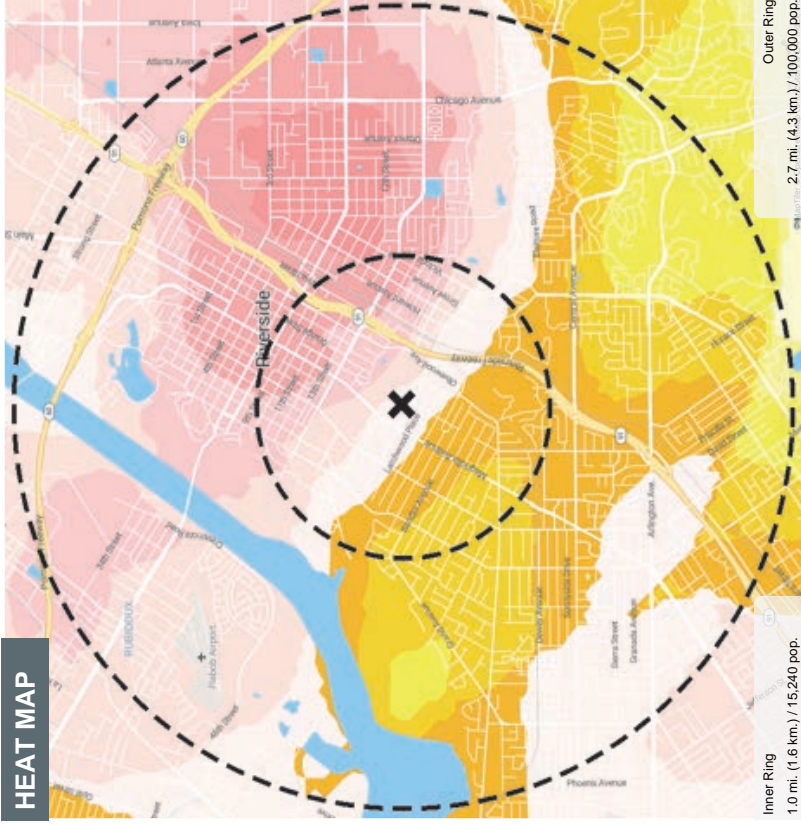
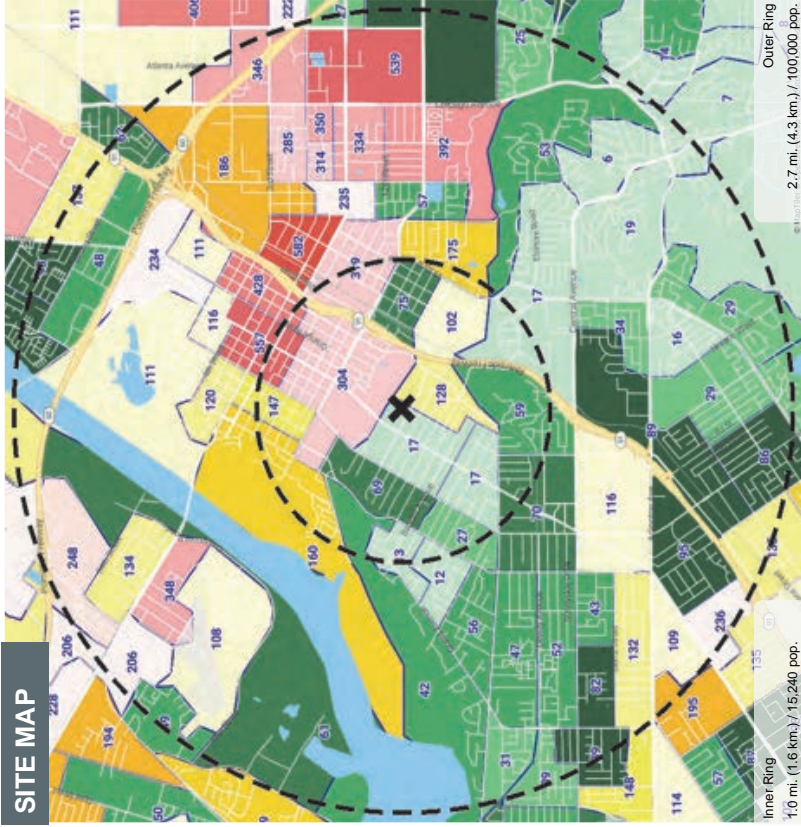
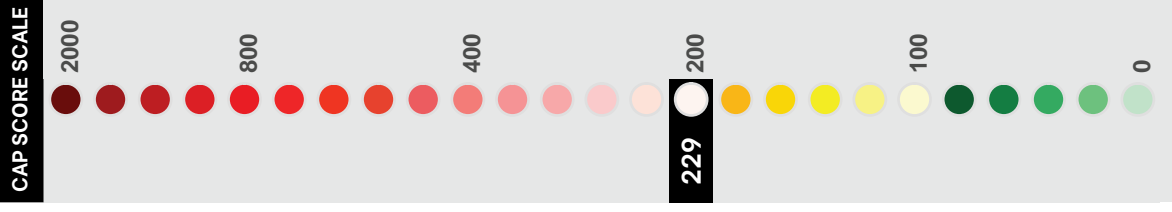
2024 NATIONAL CRIME RISK SCORES

CRIMES AGAINST PERSONS	257	CRIMES AGAINST PROPERTY	380	SUPPLEMENTAL SCORES	
Homicide	184	Burglary	408	Simple Assault	233
Rape	231	Larceny	357	Vandalism	294
Robbery	249	Motor Vehicle Theft	460		
Aggravated Assault	275				

THIS SITE'S CAP INDEX® SCORE:

229

THE CRIME RISK AT THIS SITE IS 2.29
 TIMES THE NATIONAL AVERAGE OF 100.



MAX-3 SITE MAP



SITE NAME: RIVERSIDE COMMUNITY COLLEGE
ADDRESS: 4800 MAGNOLIA AVENUE, RIVERSIDE, CA 92506

2024 NATIONAL CRIME RISK SCORES

THIS SITE'S CAP INDEX® SCORE:

229

THE CRIME RISK AT THIS SITE IS 2.29
 TIMES THE NATIONAL AVERAGE OF 100.

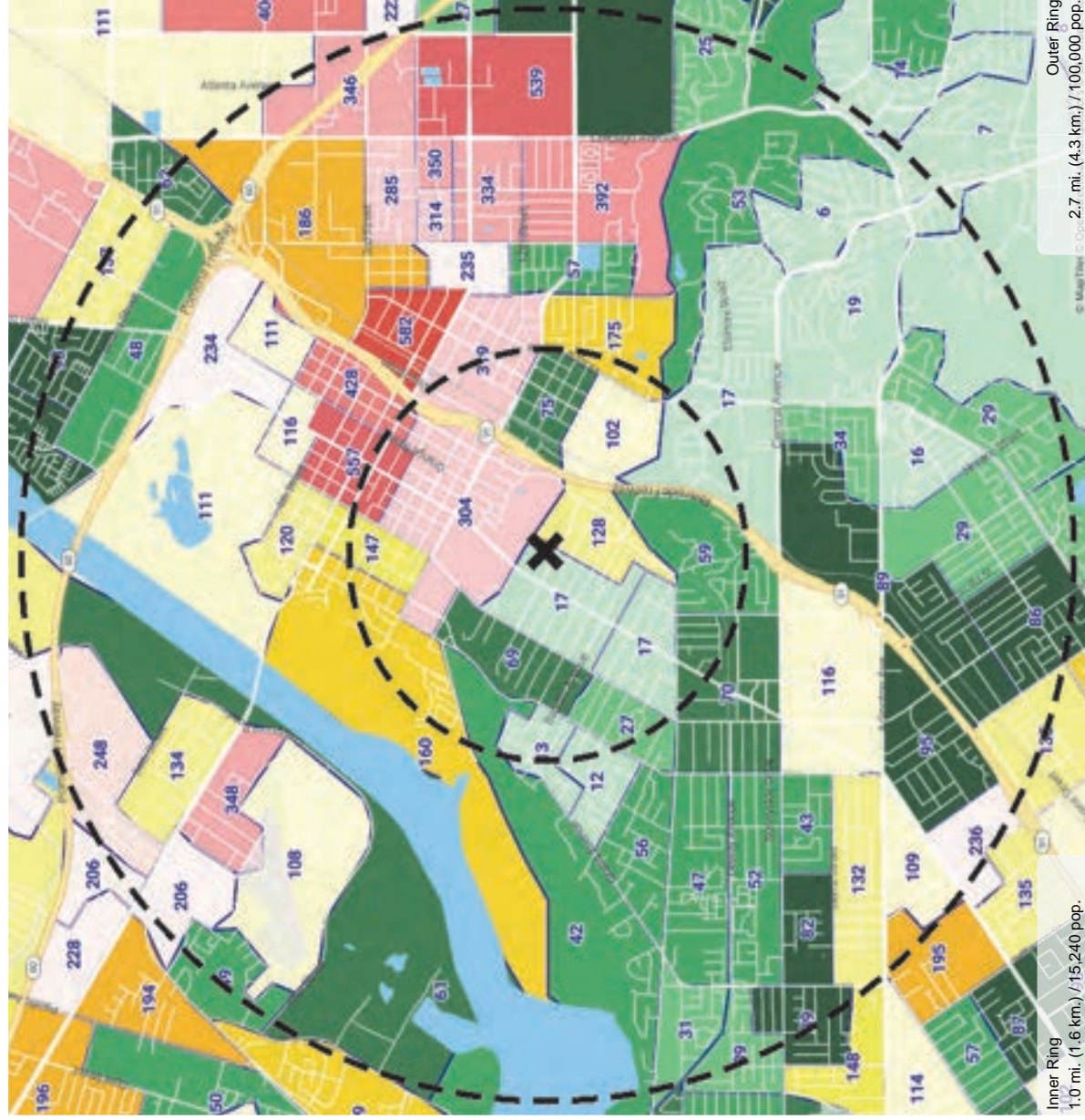
CRIMES AGAINST PERSONS 257

Homicide	184
Rape	231
Robbery	249
Aggravated Assault	275

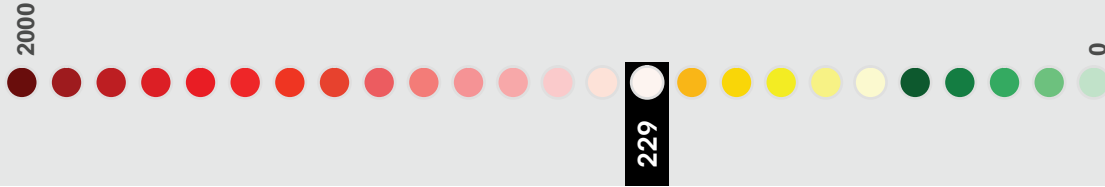
Larceny 357

SUPPLEMENTAL SCORES

Simple Assault	233
Vandalism	294



CAP SCORE SCALE



Creation Date: June 07, 2024
 Database Year: 2024

MAX -3 HEAT MAP



SITE NAME: RIVERSIDE COMMUNITY COLLEGE
ADDRESS: 4800 MAGNOLIA AVENUE, RIVERSIDE, CA 92506

2024 NATIONAL CRIME RISK SCORES

THIS SITE'S CAP INDEX® SCORE:

229

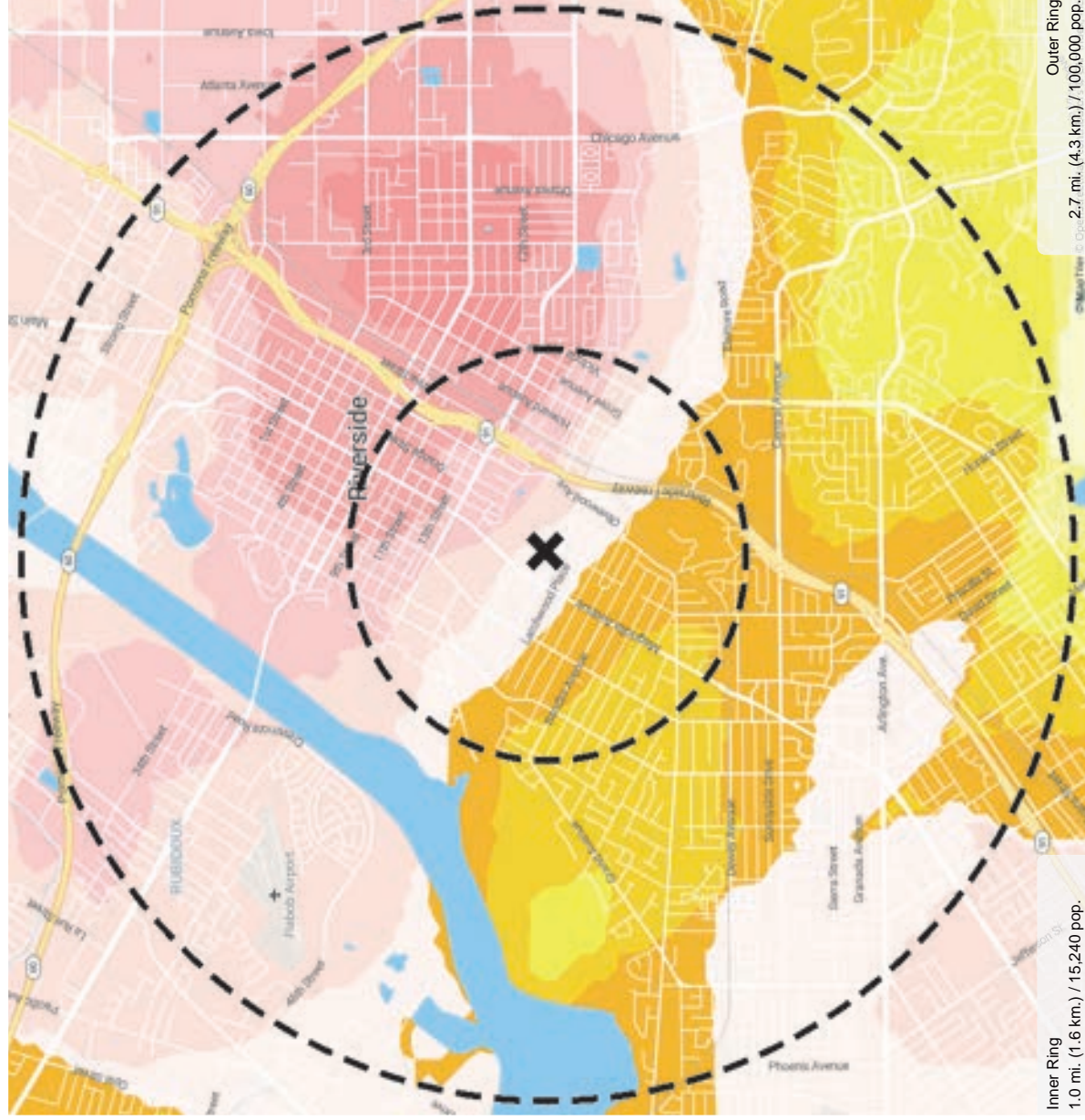
THE CRIME RISK AT THIS SITE IS 2.29
 TIMES THE NATIONAL AVERAGE OF 100.

CRIMES AGAINST PERSONS	257
Homicide	184
Rape	231
Robbery	249
Aggravated Assault	275

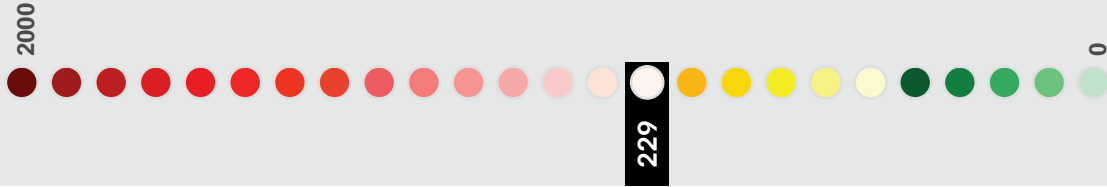
Larceny 357

SUPPLEMENTAL SCORES

Simple Assault	233
Vandalism	294



CAP SCORE SCALE



Creation Date: June 07, 2024
 Database Year: 2024

MAX - 3 SCORE SUMMARY



SITE NAME: RIVERSIDE COMMUNITY COLLEGE
ADDRESS: 4800 MAGNOLIA AVENUE, RIVERSIDE, CA 92506

The Score Summary includes a total of 108 risk scores - 12 for each of 3 geographic levels and 3 time periods. 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 State Scores compare the site to the state averages and the County Scores to the county averages. Past, Current, and Projected risk scores are provided to allow for trending.

GEOGRAPHIC LEVEL	UNITED STATES			CALIFORNIA			RIVERSIDE COUNTY		
	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029	PAST 2020	CURRENT 2024	PROJECTED 2029
CRIME RISK SCORES									
CAP Index® Score	219	229	242	184	191	205	206	210	228
CRIMES AGAINST PERSONS	251	257	259	217	222	230	207	205	214
Homicide	176	184	200	197	205	225	170	179	203
Rape	198	231	229	205	240	244	169	189	194
Robbery	238	249	267	190	196	214	230	234	258
Aggravated Assault	269	275	280	237	244	256	206	204	215
CRIMES AGAINST PROPERTY	366	380	377	314	328	338	346	367	375
Burglary	348	408	411	307	355	368	317	398	420
Larceny	360	357	352	343	344	351	388	384	387
Motor Vehicle Theft	431	460	453	229	250	259	252	277	286
SUPPLEMENTAL SCORES									
Simple Assault	228	233	265	252	260	303	202	199	232
Vandalism	275	294	314	307	336	370	275	296	325



ABOUT CRIMECAST SCORING

THE CAP INDEX® SCORING SYSTEM

The CAP Index® Scoring System uses sophisticated forecasting techniques that combine demographic and business statistics with crime and loss data to calculate crime risk. The foundation of our forecasting approach is the “Social Disorganization Theory,” which asserts that higher degrees of social discord in a neighborhood tend to correlate with higher levels of crime.



SCORING METHODOLOGIES

CAP Scores for a specific business application are generated using one of four CAP Index® Scoring Methodologies. These scoring methodologies account for the fact that perpetrators often travel varying distances to commit crimes (the “journey to crime”) depending on the target. The scoring methodologies also consider the nature and attractiveness of different types of targets for different types of crimes. Each methodology designates a progressively larger “sphere of influence” that is used to assess the risk of crime. Each sphere is defined by a maximum geographic radius or a population threshold. These spheres have different components that drive the overall crime risk score. The inner part of the sphere focuses on the nearest neighborhoods and receives the higher percentage of the weight. The outer part of the sphere considers more distant avenues of vulnerability and receives the remaining percentage of the weight.

Scoring Methodology	Outer Ring / Population for Assessment	Weight	Inner Ring / Population for Assessment	Weight
MAX-1	1 mile (1.6 km.) or 25,000 people	N/A	1 mile (1.6 km.) or 25,000 people	100%
MAX-3	3 miles (4.8 km.) or 100,000 people	20%	1 mile (1.6 km.) or 25,000 people	80%
MAX-6	6 miles (9.7 km.) or 400,000 people	20%	2 miles (3.2 km.) or 100,000 people	80%
MAX-12	12 miles (19.3 km.) or 1,600,000 people	33%	4 miles (6.4 km.) or 400,000 people	67%

CAP SCORE SCALE

CAP Scores range from 0 to 2000, with 0 representing the lowest risk and 2000 the highest; 100 is average. A score of 600 is 6 times the National Average, and a score of 25 indicates a risk that is 1/4 of the National Average.



RELIED UPON
BY OVER
80%
OF THE
FORTUNE 100

THE LEADERS IN CRIME RISK FORECASTING

CAP Index empowers organizations to make better-informed decisions throughout the security planning and security management cycle. Whether you are opening a new location, planning security measures for your existing locations, or conducting services off-site, our validated crime risk intelligence will help you create impactful security solutions to protect your customers, employees, assets, and your bottom line.



CRIMECAST® DATA & REPORTS

Quantify and visualize your risk with our detailed, industry-leading, site-specific crime risk reports.



RISK CONSULTING & ANALYTICS

Elevate your security program by having our team of consultants produce a crime risk scoring system tailored to your organization's needs.



TECHNOLOGY, PLATFORMS & MODULES

Manage your security planning process and loss prevention program from one dashboard.

HOW WE HELP: ASSESS YOUR RISK AND OUTSMART CRIME®



Make your customers, employees, and assets safer



Reduce crime, loss, and claims



Optimize the return from your security investment



Ensure compliance with industry standards



Reduce litigation and avoid adverse judgments






Protect your brand

800.227.7475 | 001.610.903.3000 | capindex.com | askcap@capindex.com


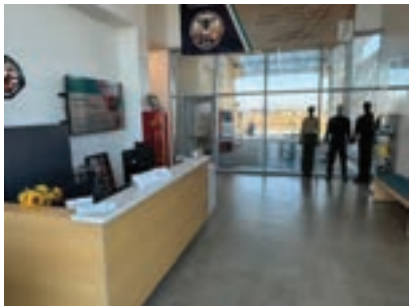





APPENDIX F - COLLEGE CAMPUS AND DISTRICT BUILDINGS
OBSERVATION AND RECOMMENDATIONS REPORTS




Ben Clark Training Center Buildings #3 & #5



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>Emergency call station towers are positioned within the West Lot parking lot and easily identifiable as the blue strobes remain illuminated at all times. All call stations with blue strobes should function with the blue light illuminated.</p>	<p>The operational state of the emergency call stations is excellent, this is best practice, and the approach should be applied to all emergency call stations across the district.</p>	0
2		<p>Cobra-head luminaires operate on motion and provide controlled lighting distribution via Light Emitting Diodes (LEDs). Placement of lighting is consistent around the parking lot perimeter.</p>	<p>General observation only. The lighting deployed is appropriate for the space use and embraces technology and lighting heads that support minimalization of light pollution.</p>	0
3		<p>Covered parking ADA spaces are clearly identified with physical and tarmac painted signage. The cover consists of solar panels, a video surveillance camera was removed during the construction process and has not been reinstalled.</p>	<p>Reinstall the removed video surveillance camera to enhance the real-time and forensic viewing capabilities.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
4		<p>Wall mounted video surveillance at the Main Center provides visibility of activity on the sidewalk. The building name and function is clearly displayed on the hanging banners. Landscaping adjacent to the building in some areas is above the recommended CPTED maximum height of 2' for ground coverings.</p>	<p>Perform schedule landscaping maintenance to maintain ground coverings below the recommended CPTED height of 2'. The landscaping is excellent but does provide some area for bad actor concealment.</p>	3
6		<p>Wall mounted cobra head sconces provide illumination of the adjacent sidewalk. Shrubbery directly below the sconce may impede intended light distribution onto the sidewalk.</p>	<p>Reference recommendation #5 regarding landscaping maintenance.</p>	3
7		<p>Goose neck mounted video surveillance camera provides visibility of pedestrian activity approaching the building from the parking lot.</p>	<p>General observation only.</p>	0
8		<p>Building main entrance does not have access control measures applied. Doors are locked and secured using brass key only. Exterior glazing has window film applied that reduces visibility from the exterior side. The film is intended for reduction of sun glare rather than a primary</p>	<p>Install access control measures on the opening providing restricted access and ability to unlock on schedule as needed. Video surveillance should be integrated with access control providing alarm event camera call-up. Install an external video intercom with master station located at the main entry desk</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		security visibility reduction perspective.	supporting ability to communicate both audibly and visually with persons requesting entry if the building is in a locked state.	
9		The building intrusion detection system is armed and disarmed locally using a security credential that is presented by authorized persons at the adjacent card reader. Access control card reader is provided for controlled entry into the North Hallway.	General observation only.	0
10		There is no remote locking capability available to the lobby desk staff to remotely lock and secure doors from the desk. Ability to communicate with persons on the public side if the building from within a secured interior is not available as no provision of intercoms.	Reference recommendation #8 regarding video intercom installation. Electrifying the entry doors and installing a remote release and or lock down button at the front desk would support immediate locked down and controlled entry as needed. Video surveillance cameras should be streamed on a monitor at the front desk to provide situational awareness of general activity.	4
11		Window treatments are installed providing ability to lower and restrict visibility from the public exterior side into the public safety space. Ground covering shrubs are above the CPTED recommended 2' height obscuring visibility of some exterior windows and supporting potential bad actor concealment.	Perform landscaping maintenance to reduce ground covering height to no more than 2'. Add additional exterior lighting and video surveillance to provide visibility and monitoring of activity during the hours of darkness.	3
12		Exterior 360 camera ceiling surface mounted. Unable to verify of the camera field of view is impeded negatively by the adjacent pole.	Review the camera field of view and verify that there is no blocking of visibility by the post.	2





ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
13		<p>The public safety center exterior is set back from the gravel area with ground covering that requires maintenance review. Window treatments are used to block sunlight and obscure visibility from the public side into the building. Fixed seating provides natural surveillance with eyes on activity when occupied.</p>	<p>Perform landscaping maintenance to reduce ground covering height to no more than 2'.</p>	3
14		<p>Controlled entry door monitored by a video surveillance camera. There is no integration between the door controls and the video surveillance camera. LED lighting provides illumination of the area during hours of darkness and several perimeter video surveillance cameras provide visibility forensically of exterior activity. Additional fixed seating areas are installed around the building perimeter with unobstructed walkways. The trash can is located within the swing of the door and could be used for propping the door open.</p>	<p>Relocate the trash can so that the temptation to potentially use to prop the door open is mitigated. Review the access control and video surveillance systems in use and determine if they can be integrated providing alarm event triggers with camera call-up.</p>	2
15		<p>Example of a lock blok in use providing ease of ingress supporting ability to close and secure a door efficiently in a lockdown when the door is in a locked state. Emergency procedures are displayed on signage fixed on the door interior side. Visibility in from the public side is not restricted.</p>	<p>Consider future installation of ballistic film that will add an additional layer of security to the existing glazing installed.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
16		<p>Access into the training center is by brass key only with no access control measures applied for controlled and audited entry. There are no exterior video surveillance cameras installed providing situational awareness of general activity or monitoring of authorized and unauthorized entry attempts. Bollards provide protection from potential vehicle impact at the HVAC units. Roof access by exterior ladder is restricted but placement of metal storage cabinets supports potential unauthorized scaling of the roof by bad actors.</p>	<p>Add access control to the building entry points providing full audit capability of persons who access the space with permission and those who may attempt entry without authorization. Add exterior video surveillance providing situational awareness and forensic viewing with integration with the access control system. Consider relocation of the cabinets to mitigate their potential misuse for scaling of the roof by providing access to the wall ladder.</p>	3
17		<p>Wall mounted sconces provide sufficient lighting during the hours of darkness. Lighting is located above each entry opening. Door hardware is storeroom function, there are no latch guards installed to restrict potential tampering and forced entry.</p>	<p>Review Division 08 standards (if available) and install latch guards at openings to restricted areas providing additional protection mitigating potential tampering opportunity for bad actors.</p>	3

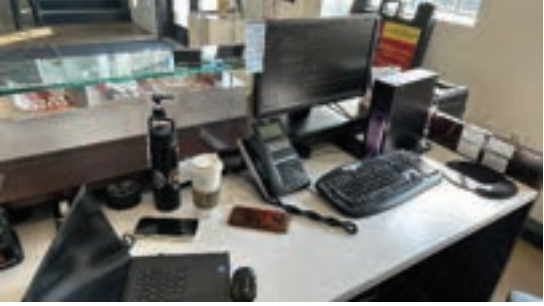


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
18		<p>The roller door located on the east side of the building is not monitored by access control door position contacts or external video surveillance.</p>	<p>Monitor the roll-up door on both the intrusion detection and access control systems. Double-pole-double-throw door position contacts would support hardwired termination to both system control panels. Installation of exterior video surveillance integrated with the access control system would support camera call-up on alarm event trigger.</p>	3
19		<p>Video surveillance cameras are installed sporadically throughout the training center interior. These cameras are used for training purpose and intent rather than for monitoring the interior space from a security perspective.</p>	<p>Reference recommendation #10 regarding provision of local video stream monitoring.</p>	3

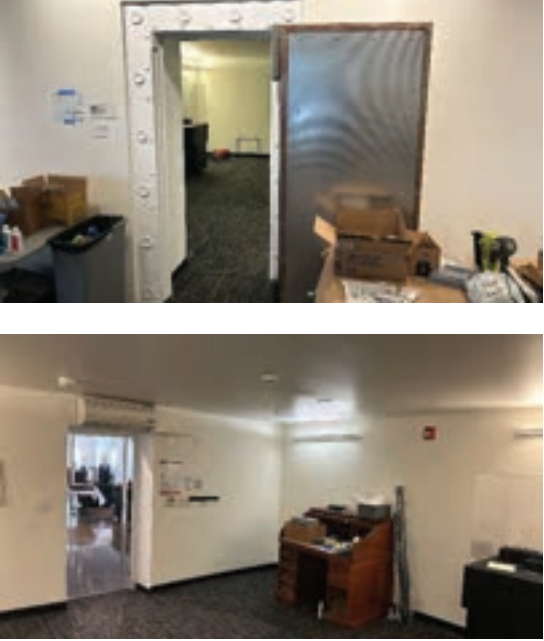
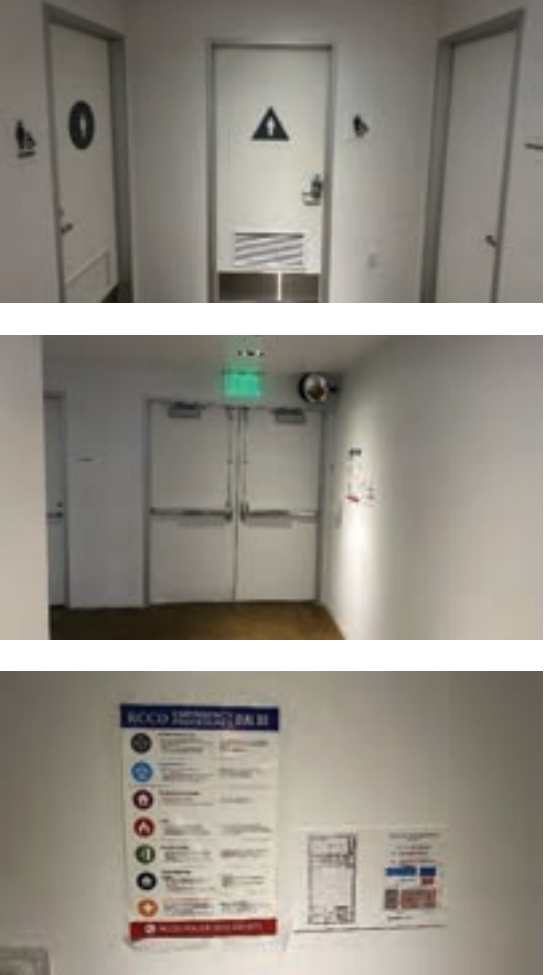
Center for Social Justice & Civil Liberties


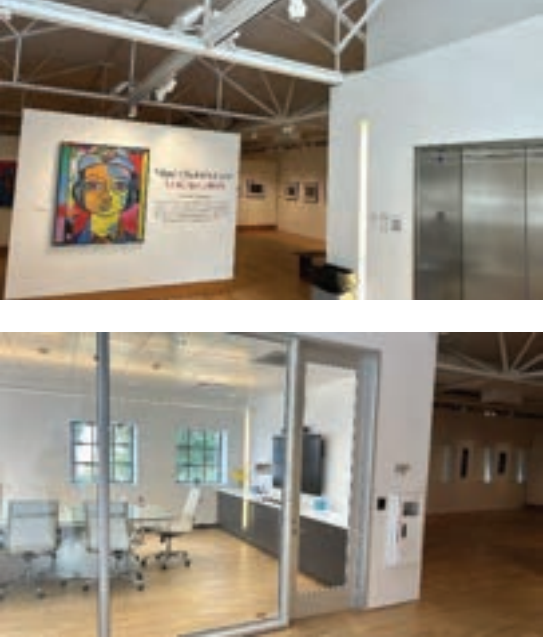
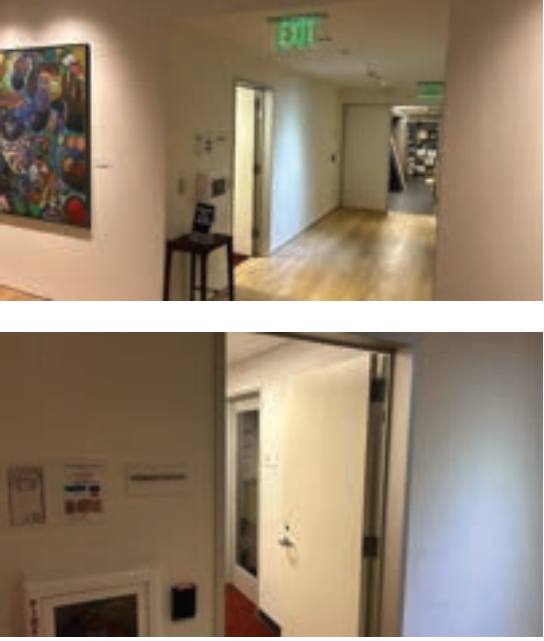
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>The exterior of the building does not have video surveillance cameras monitoring activity on the access road adjacent to the public park. There are homeless tents in the park and there have been incidents of unhoused persons entering the facility during hours of business. Low level foliage is below the 2' feet recommended CPTED ground covering height which is excellent and serves as natural territorial reinforcement of sidewalk and building. Visibility from the public side in is unobstructed when window treatments are not lowered.</p>	<p>Consider installation of additional video surveillance on the exterior for the building to provide deterrent and situational awareness and forensic review capability. Review the lighting assessment findings and install additional luminaires that provide greater illumination of the road adjacent to the park. A monitor within the building reception area should stream video camera feed for situational awareness.</p>	3
2		<p>The main entry doors are not electrified and are to remain unlocked during hours of business. There is no ability to remotely lock these doors from the reception desk or any other location. There are no window treatments applied to the glass doors reducing visibility from the public side. Doors require manually locking in a lockdown and lock blocks are not applied. Activity on approach to entry from the public side is not available on the interior as no video surveillance installed.</p>	<p>Main entry doors should be access controlled similar to the district office main entry. A remote release/locking button should be installed at the reception desk when doors are electrified to eliminate the vulnerability currently in place of mechanically locking doors in a lockdown. Consider a video intercom at the main entry providing ability to communicate with persons requesting entry visually and audibly if the building is secured due to heightened security conditions. A video surveillance camera should be installed on the exterior of the</p>	4

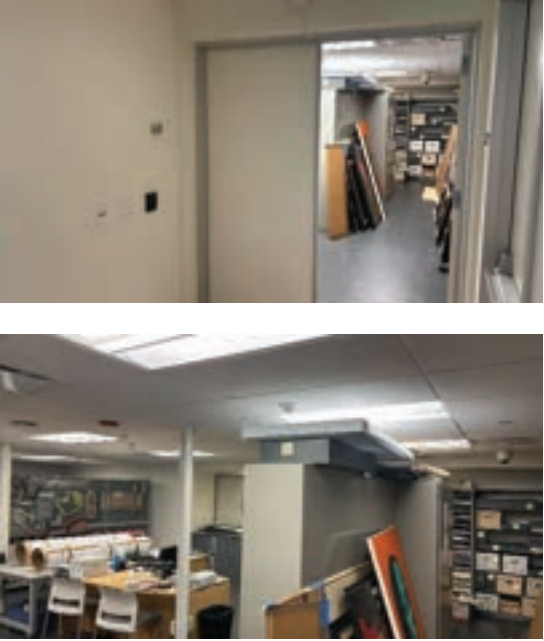
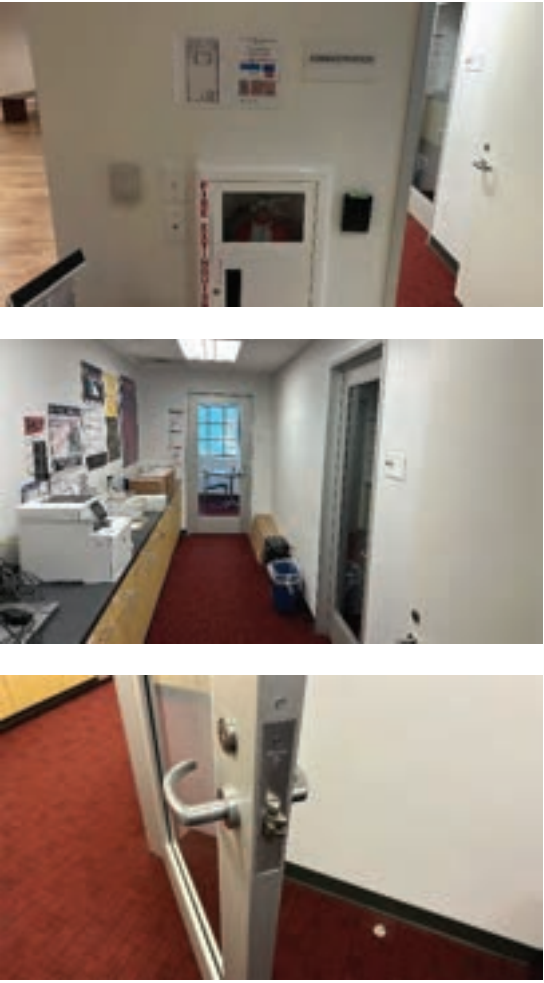
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>main entrance providing visibility of the entry approach. Consider installation of window film on all door window vision and side panels to restrict visibility in from the public side, frosted film would minimize impact on natural light and does not require to fill glazing from bottom to top.</p>	
3		<p>The DMP intrusion panel is armed and disarmed using the associated HID card reader. There are two arming stations located in the building, one at the main entrance and another at the rear entrance.</p>	<p>The use of card readers to activate and deactivate the intrusion detection system is excellent, this should be a standard approach across the entire district.</p>	0
4		<p>A video surveillance camera monitors the main entry from the interior, there is a 360-camera installed in the middle of the level one gallery space. These are the only cameras installed on level one of the building.</p>	<p>Review the need for additional video surveillance cameras to provide complete coverage of the public areas of the center. The open nature of the center to the general public justifies additional video surveillance eliminating areas for potential bad behavior to occur undetected.</p>	3
5		<p>There have been incidents of glass being smashed and vandalized. Interior window treatments are installed that can be lowered to reduce visibility from the public side in. During the hours of darkness visibility from the public side into the space can be achieved as the</p>	<p>Reference recommendation #1 regarding additional video surveillance and lighting applies. Window treatment blinds would provide better visibility restriction if black out style were installed. Glass breaks often provide false alarms, but due to the extensive amount of first</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		blinds are not blackout blinds. Glass breaks are not installed.	floor windows, there installation may be of benefit if terminated to the intrusion detection system. Glass breaks are not recommended for installation as standard across district facilities, but they do have value in specific applications.	
6		<p>Located at the reception desk there is a wireless panic button installed on the left-hand side workstation. There is only one panic button located here with the desk often occupied by more than one person. Panic buttons are tested once a year typically in August to verify if the monitoring company receives communication. Wireless panic buttons present more points of failure than hardwired and annual testing is not frequent enough to ensure that if needed they will function as intended.</p>	<p>Consider replacement of wireless panic buttons with hardwired and perform more frequent testing of the panic buttons to confirm that they communicate as intended upon activation. Install an additional panic button at the second workspace at the reception desk.</p>	3
7		<p>The main reception desk has a single telephone and two radios. The radios are used in emergency events and provide ability to communicate with the risk management team located in the district office. Floor and building captains are issued with colored vests indicating the role of the wearer.</p>	<p>Install a second VoIP telephone at the reception desk, if the desk is equipped with two workstations there should be two phones.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
8		<p>The stairwell on the right of the main entry provides an area for concealment underneath them stairs as there is no framing enclosing or gating the area off. The facility is an open public space with events occurring throughout the year during the day, the evening, and weekends. There is no security staffing provided when there are public events open to all.</p>	<p>Consider closing off of the space under the stairwell to restrict concealment by a bad actor. If the space is needed for storage install a cage/grill with secured opening. Provide district police presence or private security personnel upon request for public events. The concerns and previous experiences with agitated members of the public should be mitigated as best possible. Regardless of the building being a public welcoming facility, there is liability and care of duty that should be afforded to the district employees. Create policy and protocol that support provision of security staffing at public events.</p>	2
9		<p>A staff break room is access controlled but remains propped open frequently. The door has no door closer to ensure positive latching upon closure. The space can be used for refuge if needed, there is no secondary egress point from within the room.</p>	<p>If the space to be used for multi-purpose and general access is required, unlock the door with the double-tap presentation of a security credential. This approach will eliminate door held alarms in the access control system. Install a telephone in the space to support communications if the space is used for refuge in an emergency or lockdown.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
10		<p>The vault room door has been decommissioned with no locking mechanism currently functional. Despite this the door is heavy and has been closed before without latching requiring facilities attendance to reopen by prying with a crowbar or equivalent. If this door were closed and egress restricted, there is no ability for anyone to communicate with the outside from within as there is no telephone installed. The legacy intrusion system has not been removed; this opening is not monitored on any security electronics system.</p>	<p>Install a VoIP telephone within the vault room space providing ability to communicate out if the vault door were to be closed accidentally with no egress available. There are several spare data parts available within the room that would support the network telephone. The door should be monitored on the access control system with camera call up programmed if the door is closed.</p>	4
11		<p>The level one restrooms are set back from the main floor area within the corridor leading to the rear entry/exit vestibule. There is no video surveillance monitoring activity within the interior corridor or the access vestibule. The rear entry is outside of the controlled yard area with no ability to monitor public side activity.</p>	<p>Install video surveillance to provide situational awareness and forensic review capability of activity within the internal corridor and restroom entrance area, add an additional camera within the rear point of entry vestibule. Install a video intercom that allows for visual and audible communication with persons on the exterior who may be requesting entry. Install a spy hole in the exterior facing doors. Recommend live video stream of activity on the exterior of the opening to appear on the proposed monitor at the reception area.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
12		<p>There is no video surveillance installed on the second level art gallery area. Ability to monitor activity of members of the public both accessing the floor from the main stairwell and throughout the gallery is lacking. The conference room is access controlled and can be used by staff from the district office when needed. There is no telephone installed and no window treatment installed on the interior glass wall or door to restrict visibility from the public.</p>	<p>Consider installation of window film on all door window vision and side panels to restrict visibility in from the public side, frosted film would minimize impact on natural light and does not require to fill glazing from bottom to top. Install a VoIP telephone providing ability for communication outwards in the event of an emergency situation or lockdown.</p>	3
13		<p>The gallery archive room should remain closed and locked at all times. This archive room houses important original artwork and should be monitored as a separate intrusion detection system zone. The door was open and propped at the time of the assessment. There are two video surveillance cameras within the archive storage room, neither camera provides local video stream to the center staff workstations. There is no camera installed on the public side providing ability to monitor approach activity from the secured side.</p>	<p>Develop and implement protocol providing instruction that the archive room remain closed and locked at all times. Access into this space should be restricted by permissions and a video surveillance camera installed on the public side interfaced with the access control system. Camera call up should occur on door held, door forced, and invalid card events. The video surveillance camera live video feed should be streamed to the proposed monitor at the reception area.</p>	4


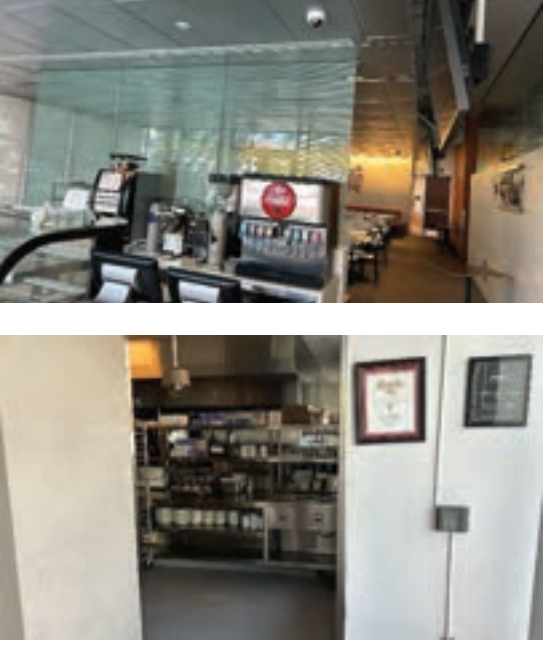

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
14		<p>Staff offices are installed within an access controlled secured corridor space, individual offices have no access control measures, lack visibility measures on the door glass, and hardware cannot be locked from the interior side. The position of the offices provides no natural surveillance or eyes on activity vision. Staff prop the door daily as they feel isolated when the door is closed. Panic buttons are installed in each office, use wireless communication, and are tested annually. There is apprehension that the single annual testing is not sufficient.</p>	<p>Provide frosted film and internal locking hardware at the staff offices. Panic buttons should be hardwired, and more frequent testing of the buttons is encouraged to allay staff concerns regarding confidence in the panic buttons to function as intended if activated. Past events with agitated members of the public have resulted in staff deescalating incidents themselves, rather than activating the panic buttons, as concerns regarding response time to requests for help are present. Install a video monitor in the office corridor providing the same video stream as that to be displayed on the proposed reception monitor. Install a lock blok on the corridor-controlled entry, the door should remain in a locked state at all times.</p>	3


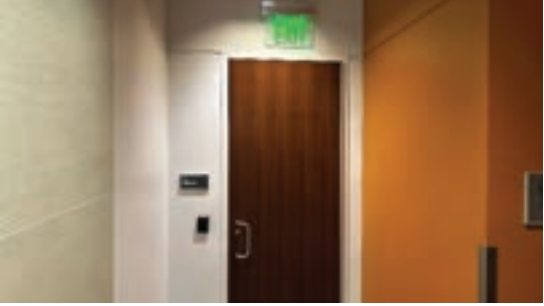
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
15		<p>Access to the second level from level one is always available from the stairwell side as the entry door is equipped with a passage trim remaining unlocked. Lack of video surveillance fails to support both real-time situational awareness and forensic viewing. The lack of card reader on this entry from the stairwell fails to provide ability to monitor entry activity via an audit trail in the access control system. There is no 'Exit' sign above the door indicating a path of egress from level one. This opening is similar to the main level one building entry doors with lack of access control technology in use, eliminating the ability to track access via an audit report.</p>	<p>Install video surveillance on the stairwell side to monitor approach from level one. Review the path of egress with the AHJ, if permitted add a card reader to the stairwell side of the door. Free ingress, if possible, should be removed as this opening leads directly to the staff office space and archive room-controlled entry point. Develop protocol that facilities and maintenance staff use their security credentials to enter the building and secured spaces rather than using a brass key. There should be an audit trail of all persons entering the building and rooms when secured.</p>	4

Culinary Arts Academy & Riverside Community College District Office

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>Dining Room access is only available during the stated hours of operation. There is no access control applied to the opening and brass key is required for entering from the exterior when the doors are locked. Exterior floor to ceiling glazing is double paned and horizontal lining film helps restrict visibility inwards. We were notified of significant damage occurring to glazing frequently and replacement required. Bollards at the junction of University Ave. and Market St. provide physical protection from potential vehicles mounting the curb. Determination of if the bollards are K-rated or not is unknown.</p>	<p>Recommend that access control be applied to the opening to support remote lockdown. Regards glazing, ensure that glass in high-risk areas is designed in accordance with relevant standards and to meet the security requirements of the threat(s), threat locations and vulnerabilities of the risk assessment. Reference: American Society for Testing and Materials (ASTM) F 1642-12 (current version) "Standard Test Method for Glazing and Glazing Systems Subject to Air Blast Loadings." Consider installation planter boxes adjacent to the glazing to serve as a setback from pedestrians to the building perimeter.</p>	2
2		<p>Exterior glazing along the University Ave. side of the building. Vandalism frequently causes damage to the glazing, there is no setback between the glazing and the sidewalk which may deter acts of vandalism. Bollards are not installed along the sidewalk.</p>	<p>Reference recommendations #1 regards glazing. Consider bollards along the edge of the sidewalk as protection against vehicles potentially mounting the curb.</p>	2
3		<p>Access from Market St. into the Culinary Arts Academy is through the District office main point of entry. This opening is opened on schedule during normal hours of operation, an internal card reader when presented with an authorized security credential will relock the doors. Axis video surveillance camera provides visibility of activity on the exterior of the opening. The RCCD Community Safety Officer</p>	<p>General observation.</p>	0

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>positioned in the School for the Arts parking garage has viewing rights to monitor cameras.</p>		
4		<p>Door remains propped open and unlocked in the path of egress when members of the public are using the cafeteria. This provides significant risk to other building and department occupants as access control programming unlocks other controlled openings allowing free path of travel throughout the entire first floor of the building. There is no video surveillance installed in the dining room corridor that supports monitoring of activity in this area.</p>	<p>Consider closing the door during normal hours of operation maintaining free egress in the event of an emergency. Provide a video surveillance camera in the corridor with visibility of activity at the reception desk. Review the existing card reader deployment and need for complete unlock, is there opportunity to reduce public access into back of house and learning areas?</p>	4
5		<p>Members of the public use the restrooms located in the District Office lobby when the dining room is in operation. The lack of dedicated dining room restrooms presents vulnerability to other building users specifically on level one as dining room users can easily access student learning areas as the path of egress from the lobby area provides unsecured openings that can easily be accessed. The dining room has minimal video surveillance installed to monitor activity. Window treatments are installed and can be used to restrict visibility from the exterior side as needed.</p>	<p>Install video surveillance to monitor general activity when members of the public use the space.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
6		<p>Glass breaks are installed on the ceiling of the dining room and are terminated to the intrusion detection system. There is no interface of glass breaks with video surveillance to support visibility of activity if an alarm event is triggered by a glass break.</p>	<p>Interface the security electronics systems to provide camera call-up in the event of an alarm event trigger. Utilize the existing security electronics to support security staffing measures and district police.</p>	2
7		<p>Open access to the kitchen from the "to-go" waiting area is concerning as it allows unrestricted access to kitchen staff and students, plus dangerous equipment such as knives. There is no counter that would provide a physical barrier between staff and students and members of the public. Open access to the kitchen area is also available on the other side of the kitchen from the corridor. Video surveillance cameras are installed behind the transaction counter and monitor the point of sales and area where public enter the space.</p>	<p>Install a counter that serves as a barrier between members of the public and students, faculty, and staff. Access into the working kitchen area should not be available to members of the public.</p>	4
8		<p>The Culinary Arts Academy is monitored with an intrusion detection alarm that is its own zone. When disarming at the Software House arming station the entry doors to the District Office are also disarmed. Video surveillance coverage of activity on the interior of the space is provided by a fixed dome Axis camera.</p>	<p>Review the zoning of the intrusion detection system, do the main administration entry doors need to be unmonitored when the culinary zone is disarmed?</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
9		<p>Ability to call the elevator requires a security credential be presented at the card reader adjacent to the elevator call button. Ability to call an elevator is permissions based through access control system programming.</p>	<p>General observation.</p>	0
10		<p>The opening accessible from the District Office level one lobby area is unlocked on schedule. This opening has an exit sign above it and should provide egress at all times which by its very nature allows access to the corridor space beyond the opening. Allowing general public access to areas that are designated for student learning is a vulnerability in the current security posture of the space. Controlled openings throughout level one provide unrestricted access, a review of the operational application of unlocking doors on schedule should occur. Additional openings may be required to restrict access to learning areas that does not impact the path of egress.</p>	<p>Reference recommendation #4 regarding the operational state of the first floor. Due to the building housing the district administration, more robust control of access should be considered.</p>	4

CULINARY ARTS ACADEMY & DISTRICT OFFICE (CAADO) BUILDING

1st Floor

Floor Captain Assignment Map

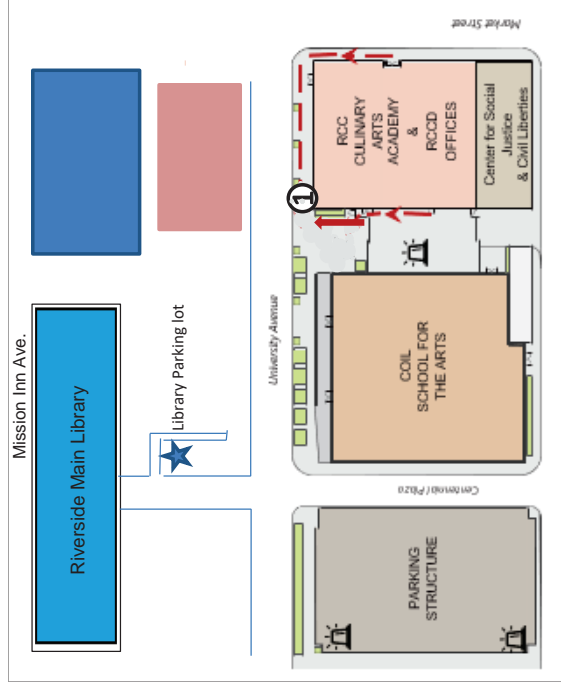
- Floor Captain | Zone 1-1
- Floor Captain | Zone 1-2



Primary Evacuation Assembly Area:
In front of Culinary | University Ave.



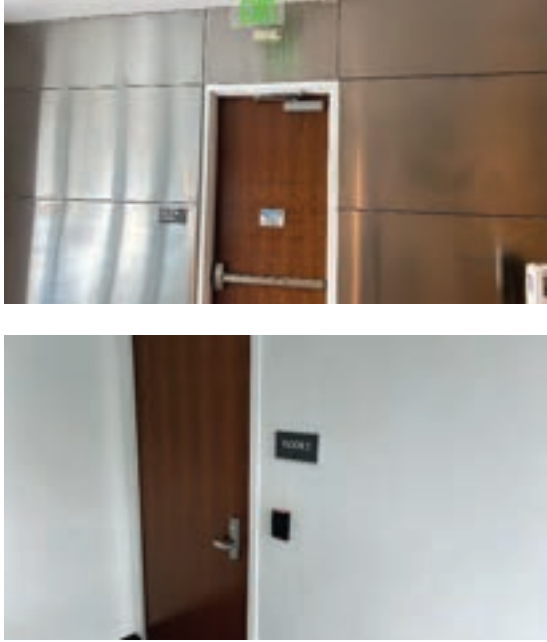
Secondary Evacuation Assembly Area:
City of Riverside Library Parking Lot | University Entrance




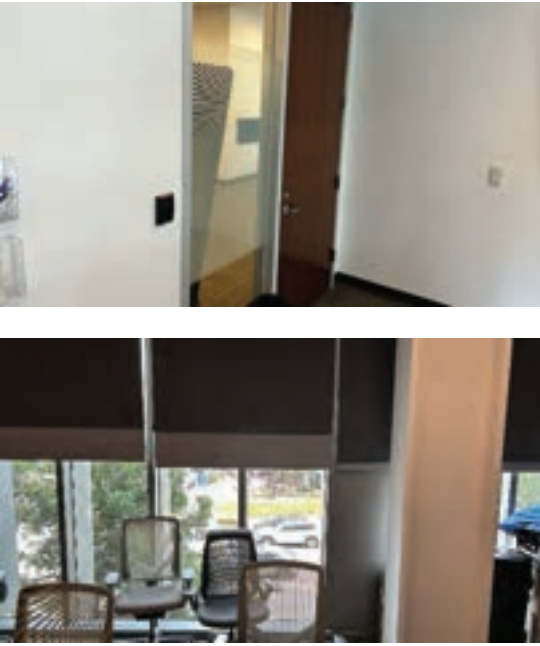
Emergency supplies

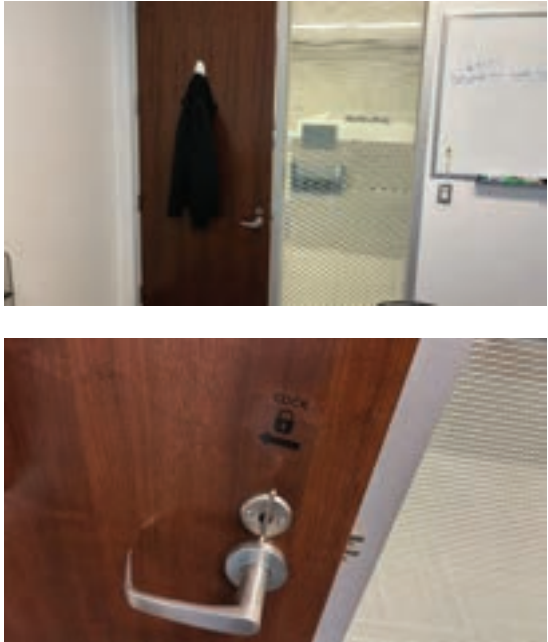
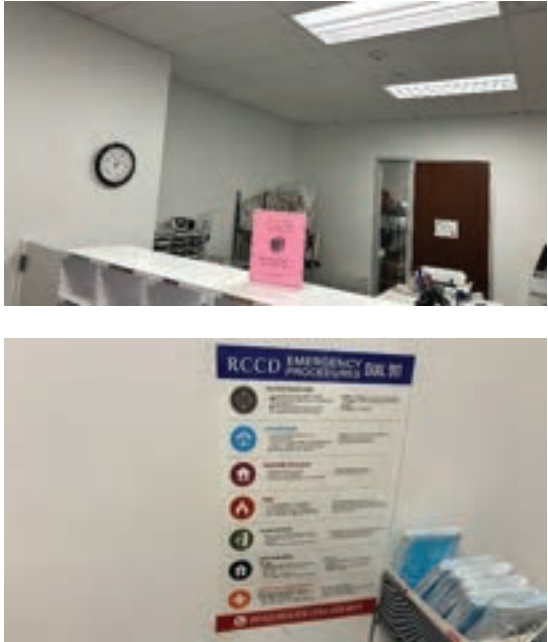
District Office

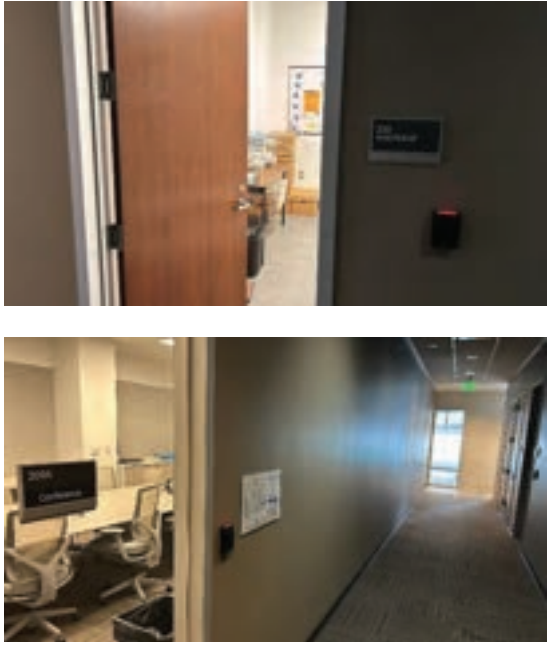

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>Main building entry doors remain unlocked during normal hours of business and can be locked using a switch at the reception desk. Access control card reader is applied to the main entry, this is not consistent with the Culinary Arts Academy and Social Justice main entry points which have no security electronic access control measures. Axis video surveillance cameras monitor activity in the main lobby area. A Software House intrusion detection arming station is located within the lobby, this arms/disarms the entire first floor. Each floor/level has its own intrusion arming station. The elevator hall call buttons require presentation of an authorized security credential to call the elevator from level one.</p>	<p>Consider installation of a video intercom to provide visual and audible communication with persons on the public side prior to granting access if the building is placed into a locked state. Conduct visitor screening in the lobby prior to providing visitors access to controlled upper floors. All guests should be met at the lobby rather than provided elevator access and sent up to the floor of the person meeting. Install video surveillance in all elevators both freight and public. Install exterior video surveillance and an internal viewing monitor to provide visibility of activity on approach to the main entry.</p>	3
2		<p>Reception desk has a wireless panic button installed underneath it that communicates directly out via the intrusion system to the Riverside County Sheriff Dispatch. There is no integration between security electronics providing instant visibility of the activation point using video surveillance. A VoIP telephone is provided at the reception desk. At the time of the assessment the staff member was uncertain if RAVE Alert mass notifications are programmed to appear on the screen located in reception.</p>	<p>Develop security design standards that provide consistency and governance to installation of devices such as panic buttons. Consider use of hardwired devices rather than wireless, wireless communication can often be impacted by the built environment; and continual review of battery life often required. Standardization of approach eliminate risk and vulnerability that ad hoc placement of devices presents. Review the screen/monitor and interface with AV systems to</p>	3



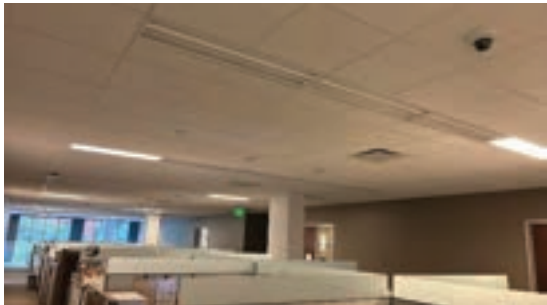
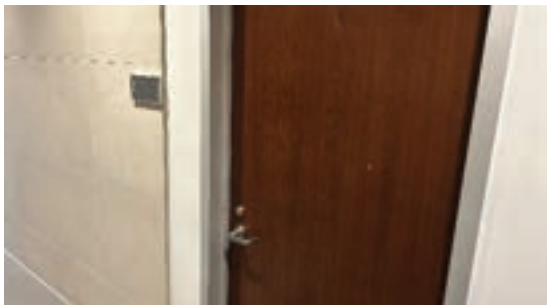
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>support Rave Alert notification display.</p>	
3		<p>Authorized security credential is required to access all floors above level one. The elevator has a card reader that upon presentation of an approved credential will energize the elevator pushbuttons and access to upper floor elevator landings can be achieved. Every authorized member of staff who works in the building has approved permissions to use the level one hall and elevator cab card readers. Permissions control of access is applied to the remainder of the building space driven by department function. Video surveillance camera are installed on each level monitoring the elevator lobbies.</p>	<p>Reference recommendation #1 regarding elevator use protocol for visitors and consideration of video camera installation.</p>	2
4		<p>Free egress is always maintained out into and through the stairwells. Stairwell doors have access control measures on the stairwell side of the opening. All members of staff have ability to reenter floors using their security credentials. Lack of security credential requires exiting of the building on level one. Axis video surveillance cameras are installed monitoring each stairwell landing and provide visibility of pedestrian activity from the top floor down. There is no integration between security electronics systems.</p>	<p>Install signage within the stairwells that informs those without credentials that egress through the first floor is required. Consider future systems integration allowing camera call-up capability when door forced, or door held alarm events are received within the access control and intrusion detection systems. Provide video camera visibility at the reception desk.</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
5	  	<p>The Human Resources (HR) department entry opening is unlocked on schedule and can be double tapped using a security credential with permissions to lock /unlock. There is a panic button installed at the department reception desk, this button as with the level one reception desk is wireless. The employee at the time of assessment was unaware of the panic button installation and planned response if activated. There is no window film applied to either of the HR access doors to restrict visibility if in a lockdown. The HR working offices space is further controlled entry with access control card reader restricting access via system permissions programming. There is a doorbell that provides ability to notify the secured space occupants that entry is requested. There is no prescreening communication tool or video surveillance installed within the HR lobby area.</p>	<p>Consider installation of a video intercom to provide visual and audible communication with persons on the public side prior to granting access if the department entry is placed into a locked state. Consider installation of window film on all door window vision and side panels to restrict visibility in from the public side, frosted film would minimize impact on natural light and does not require to fill glazing from bottom to top. Install a video surveillance camera in the reception area and provide real-time visibility of activity by monitor installed within the secure department space. Develop security design standards that provide consistency and governance to installation of devices such as panic buttons. Consider use of hardwired devices rather than wireless, wireless communication can often be impacted by the built environment; and continual review of battery life often required. Provide and document panic button awareness and use training of employees that may be stationed at the reception desk.</p>	3

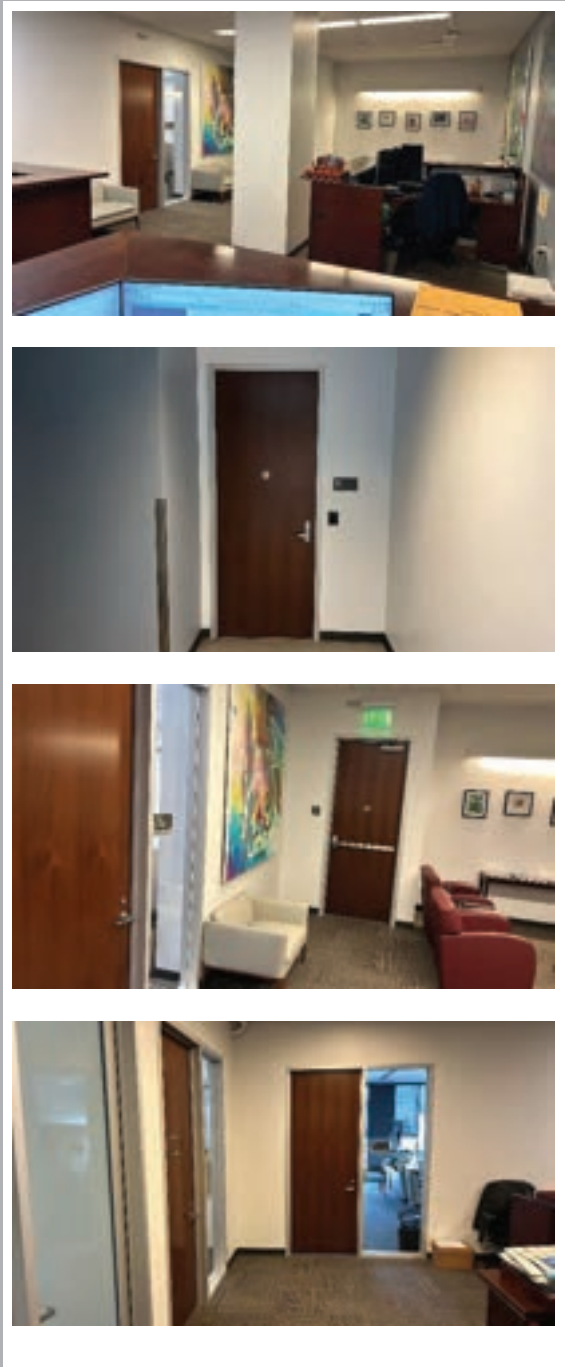
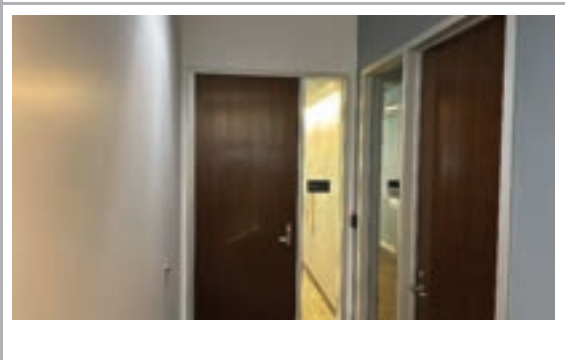
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
6		<p>Floor Captains are provided with blue vests that clearly identify their role in an emergency situation. Walkie-talkies are also provided and serve as the primary communication tool in an emergency. Each workstation has a VoIP telephone, emergency procedures are well distributed throughout the building.</p>	<p>General observation. Identify a floor captain or marshal who is responsible for each floor or tenant of the site (whichever is more applicable). The captain or marshal is responsible for implementing each floor's or tenant's appropriate emergency plan and ensuring that it is carried out properly. In the case of evacuations, check for stay-behinds. Ensure that all persons of responsibility are provided appropriate attire to wear in an incident response situation. Locate and address the needs of people who require special attention during a disaster (e.g., the disabled, non-English speakers, etc.).</p>	0
7		<p>The conference room accessible from the HR department reception area is locked at all times and requires a brass key to enter from reception. Free ingress is available from the secured office side. There are access control measures applied to the door on the interior of the conference room that provides direct access back into the HR department. There are no egress signs installed above either opening indicating the approved path-of-travel. An egress sign may be required above the door leading back into the reception area. Verification with the AHJ would determine if needed. Window treatments are installed on the exterior windows and</p>	<p>Consider installation of window film on all door window vision and side panels to restrict visibility in from the public side, frosted film would minimize impact on natural light and does not require to fill glazing from bottom to top. Refer to AHJ reference application of 'Exit' signs, it is impossible for a non-authorized credential holder to egress into the secured space, the only egress option without special knowledge for the public is through the conference room entry door from the reception area.</p>	3

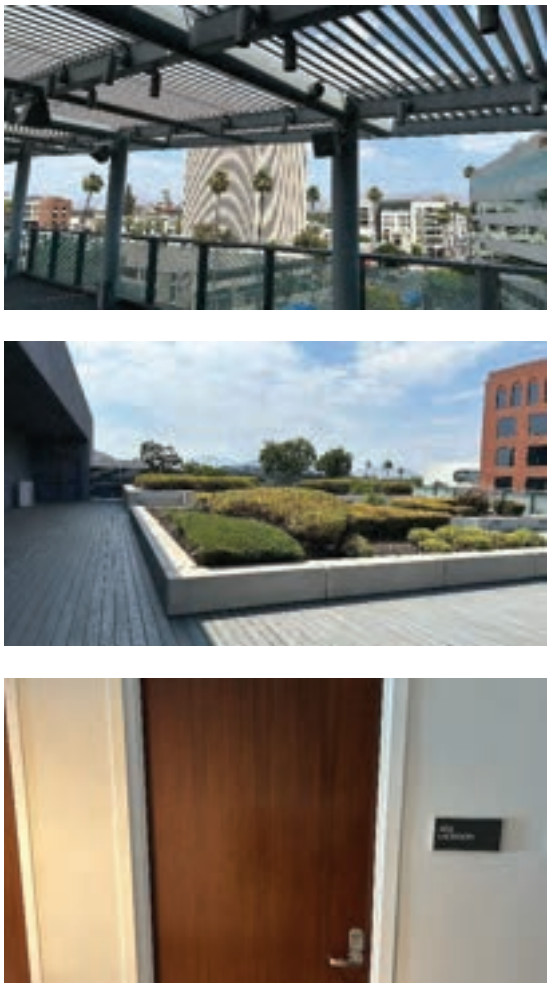
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		frosting on the interior glazing does not deter visibility.		
8		<p>This office in the HR department is typical of offices throughout the building. There is window film applied that obscures visibility when the lights are not turned on, but when the lights are turned on visibility is unimpeded. Window treatments are installed on the exterior windows and can be lowered as needed; primary intent above level one of the treatments is to reduce sun glare. The office door can be locked from the interior by throw of a thumb turn lever. The secondary departmental access door leading into the HR suite maintains free egress and has access control from the public side.</p>	<p>Reference recommendation #7 regarding use of frosted film that restricts visibility into office spaces. Review the application of the sticker on the interior of the offices. Verify that the directions given match the function of the hardware.</p>	2
9		<p>Access into the mailroom on the second floor requires presentation of an authorized permission security credential. Everyone with access permission into the building can enter the mailroom. There is no door closer installed ensuring that positive latching of the door occurs each time the door closes after egress. Closers should be installed at all access control openings as a standard. There is no video surveillance camera installed in the mail room which may contain personal staff mail. The corridor providing access to the conference rooms is dark with lighting appearing to be emergency lighting turned on only. There is no video surveillance monitoring activity within the corridors and the approach to the mailroom. All openings have access control measures applied which is excellent.</p>	<p>All access control doors should have door closers installed on them as standard, this should be captured within security design standards. Consider installation of video surveillance camera both within and outside of the mail room. Ability to monitor activity in a space that may contain personal documents should not be seen as an infringement on privacy. The access to all approach indicates that the space is a communal space rather than private working office. A camera on the public side of the room provides observation of approach and a multi-sensor camera would capture general corridor activity. Corridor lighting should be turned on at all times during normal hours of business.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
10		<p>The Cashiers Office is located on the second level and is nondescript with no signage outside drawing attention by indicating the function of the space. Access into the room is by restricted permissions-based access control security credential. The space is an independent zone on the DMP intrusion alarm system and is armed by the space users whenever they are leaving the room unoccupied. Approximately \$5000 float is carried, and monies are collected by a contracted courier Monday, Tuesday, Wednesday, and Thursday each week. Couriers also bring funds from each of the district college campuses into the central district space. The courier has an access control credential that provides access into the secured courtyard, and into the building but not directly into the cashier's office. Office occupants can physically observe the arrival of the courier from the second-floor window. There is a video surveillance camera installed within the office but no</p>	<p>Consider providing hardwired panic buttons at both staff members desks. Provide radios for communication with floor captains over a dedicated radio channel in the event of a lockdown or other emergency, rather than reliance on personal cell phones if the network telephones lose power. Recommend a monitor be installed within the room providing live video stream from the camera monitoring the room entry door from the public side; allowing visibility of room occupants to observe person(s) requesting entry.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>visibility of activity on the exterior of the approach to the office from within. The existing spyhole has limitations in visibility provided. A single wireless DMP lockdown button was observed in the space, this is not fixed to a desk or wall and is tested annually. Cashiers Office staff do not have walkie-talkies/radios for use in the event of shelter-in-place or lockdown. If the building network was compromised, and the VoIP telephones were out of service, there is reliance on personal cell phone to communicate outwardly.</p>		
11		<p>Each floor has its own Software House arming and disarming station for the intrusion system. The only separate zone within a floor is the Cashiers Office.</p>	<p>The existing process and protocols in place regarding the intrusion system are logical. A review of the first-floor arming station and associated zones is recommended as understanding is that the entire floor is disarmed/armed including the Culinary Arts space.</p>	1
12		<p>Video surveillance cameras observe stairwell activity from the secured side on each floor. This typical standard approach is excellent, there is no integration between systems to support camera call-up on alarm event i.e., door held, or door forced.</p>	<p>The standard approach of camera layout at each stairwell is good and reflects typical security electronics design practices. Consider future systems integration allowing camera call-up capability when door forced, or door held alarm events are received within the access control and intrusion detection systems.</p>	1
13		<p>Room BDF 205 is a building distribution framework critical infrastructure room with brass key access only. Typically, critical infrastructure best practice is to secure such rooms with access control; and monitor both the public and secured sides with video surveillance. There is no ability to audit check who has</p>	<p>Critical infrastructure rooms typically receive robust security measures and do not rely on brass key as the primary means of access. Across the district college campuses there are many data rooms that are accessible by access control card reader only, it is recommended that this same approach be adopted at</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>accessed or attempted without permission the space. There is a lack of standardization across the district regarding application of access control at critical infrastructure rooms.</p>	<p>the district office. Access control will provide ability to authenticate approved access and use of multi-factor authentication is also an additional security option. Additionally, the current brass key access mode does not provide an audit trail of when the room is entered. A video surveillance camera should be installed both internally (was unavailable to observe) and within the corridor and interfaced with the access control system.</p>	
14		<p>The main entrance into the Chancellor's Suite/Executive Offices on the third level is controlled with an access control card reader. This card reader is placed into an unlocked state and free entry provided to all. There are concerns with this raised by the reception staff as they have no ability to remotely lock the door or observe approach activity on the exterior of the suite. There are no video surveillance cameras installed within or on the exterior of the suite with direct focus providing visibility of activity. Wireless panic buttons are installed at the reception desks and within the individual executive office spaces. Ability to communicate with persons requesting access if the main suite door was locked is no available and reception staff must open the door to engage prior to granting entry. The lack of options to restrict access presents risk at such a high-profile space.</p>	<p>The Executive Suite is a prominent space that contains high profile district officers. Concerns of support staff should be considered, and measures put in place that allow for ease of safety and security concerns shared by staff. Consider installation of a video intercom at the main suite entry providing visibility and ability to vet people prior to providing access. Consider installation of a video surveillance monitor that provides video stream of the first-floor reception area, and additional elevator landing cameras. Install a camera above the suite waiting area and stream video to the proposed monitor. Replace wireless panic buttons with hardwired and provide remote locking and release of the suite entry door at both reception desks. Engage the reception staff regarding concerns relating to the existing open free ingress operational state.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
15		<p>Access into the Chancellor's Suite is controlled with access control card reader from the general working space. There is no camera installed monitoring activity of approach to the Chancellor's Suite. Cameras are installed on each floor monitoring the stairwell egress points from the secure side.</p>	<p>Reference recommendations #14 regarding additional video surveillance and monitoring suggestions.</p>	4


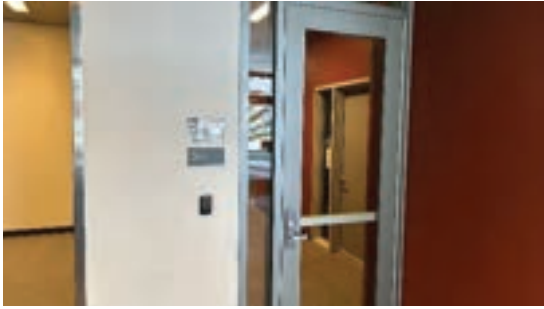


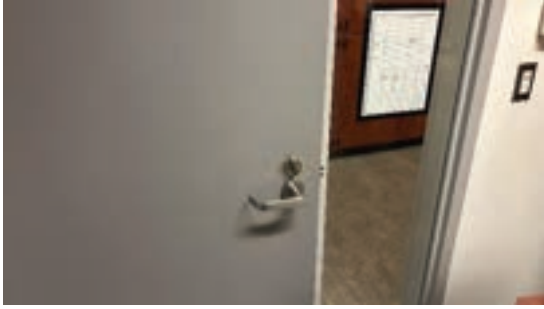
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
16		<p>Access to the rooftop entertaining area is controlled with card reader. A single exterior video surveillance camera monitors the activity onto the roof from the stairwell. There is no video surveillance installed to monitor general rooftop activity. The security electronics systems are not integrated to support immediate visibility via camera call-up if a door forced or door held alarm was received. The lactation room has a privacy indicator installed which is excellent.</p>	<p>Additional video surveillance should be provided to support situational awareness of activity on the rooftop. Security electronics system standards should be created, and systems interfaced.</p>	2

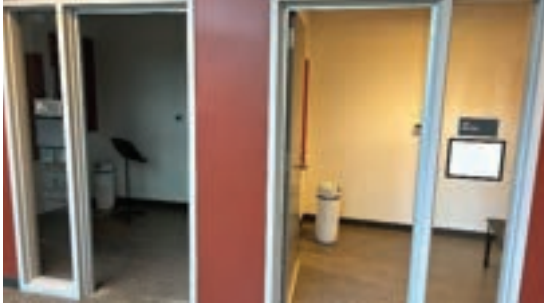

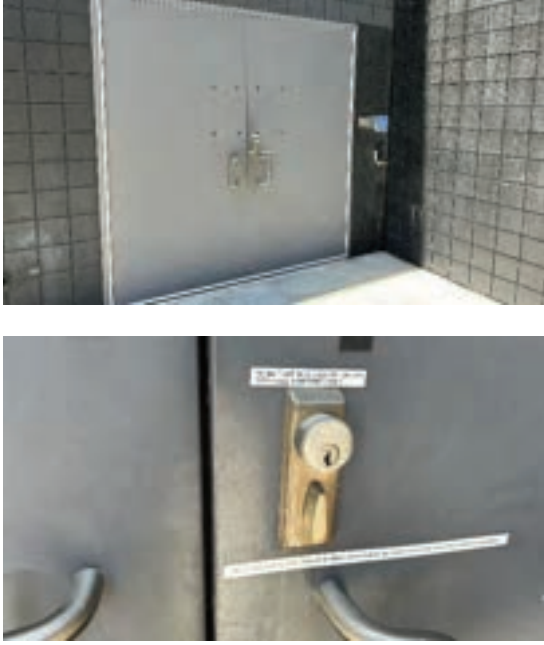
Henry W. and Alice Edna Coil School for the Arts




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>The main entry doors do not have access control measures applied to them and a brass key is used for entry by faculty. The doors are electrified and can be unlocked by activation of a remote release button at the lobby desk. The doors are monitored on the intrusion detection system only. Faculty raised concerns that the doors on the front of the lobby do not positively latch each time upon egress, this leaves the building vulnerable to unauthorized entry. There is no ability for communication with the public side from the secure prior to activation of the remote release as there is no video intercom installed. The opening is monitored by an Axis video surveillance camera on the public side. Vandalism and damage to glazing results in replacement of double-glazed panes at \$9,000 each. Faculty have both keys and access credentials to enter the building which is an ineffective approach to applying security measures to the building.</p>	<p>Recommend that access control be applied to the opening to support remote lockdown. Apply a video intercom with communication to a master station at the entry desk to allow controlled access as needed. Access by Faculty should be by security credential only. Review the closing mechanism and ensure positive latching of the doors on closure. Regards glazing, ensure that glass in high-risk areas is designed in accordance with relevant standards and to meet the security requirements of the threat(s), threat locations and vulnerabilities of the risk assessment. Reference: American Society for Testing and Materials (ASTM) F 1642-12 (current version) "Standard Test Method for Glazing and Glazing Systems Subject to Air Blast Loadings."</p>	4
2		<p>Glass breaks are installed on the secure side of the lobby on the ceiling approximately 16 feet apart from each other. The lobby is also monitored with video surveillance cameras, these cameras are single fixed dome manufactured by Axis. The building's intrusion detection system can be armed and disarmed at the Software House arming station located on the office wall.</p>	<p>General observation. Recommend that security electronics systems interface to support camera call-up on alarm event trigger and support security operations and personnel.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
3		<p>The main concert hall is equipped with lighting on the side of the seats that support visibility when lighting is lowered. There is emergency lighting within the concert hall, but no public address system. Faculty requested that video surveillance cameras be installed within this space to provide visibility of activity both from a situational awareness perspective and forensically. This request has previously been made but this miss on the basis of cost.</p>	<p>Install video surveillance to support observation of activity and forensic review of concert hall use. Consider an internal public address system supporting ability to provide public notification of communications/announcements. Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions.</p>	3
4		<p>The monitor in the lobby area displayed an alert that the RAVE notification system had performed a test. The information displayed provided guidance so those who may or may not have received the alert through the mobile application. Guidance was provided for those who</p>	<p>Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. Consider use of monitors at other locations in public areas to communicate</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>did not receive the notification with direction on how to find the RAVE app on the Google and Apple stores. Mass notification alerts issued to cell phones require the RAVE application and faculty and staff to opt in. The image of the messaging on the cell phone displays the communication issued June 26, 2024.</p>	<p>RAVE alerts and application opt-in instructions.</p>	<p>5</p>
<p>5</p>		<p>The two openings in the lobby area identified as emergency egress openings have issues with the doors positively latching upon closure. There appear to be issues with the door closers that is impacted by ADA code compliance resulting in doors presenting risk as unauthorized access can be achieved when the doors are not secured. There are no local door alarms that annunciate when egress has occurred at these openings.</p>	<p>Review the doors and perform corrective action to support positive latching upon closure. Consider 24 VDC electrified door closers subject to code compliance to provide additional closure support as needed. Consider installation of local door alarms that annunciate on unauthorized opening of doors. Local alarms with key switch can be turned-off during events to eliminate nuisance alarms.</p>	<p>5</p>
<p>6</p>		<p>Access to the box office requires a security credential be presented at the access control card reader. Activity within the box office is monitored by a video surveillance camera. The stairs leading to the second level present vulnerability during an event, as access through this stairwell provides opportunity to gain entry to controlled access areas on level one by navigating level two and using the second stairwell to access level one. Faculty advised that during public events this stairwell is supervised to restrict public access.</p>	<p>Review the stairwell access measures on the second level landing. Securing access to the second level mitigates the current concerns raised by faculty regarding access behind locked and secured space on level one using the open stairwell. Access could be provided as operations require on schedule, apply remote lockdown capability to support compartmentalization of the building in a lockdown.</p>	<p>4</p>

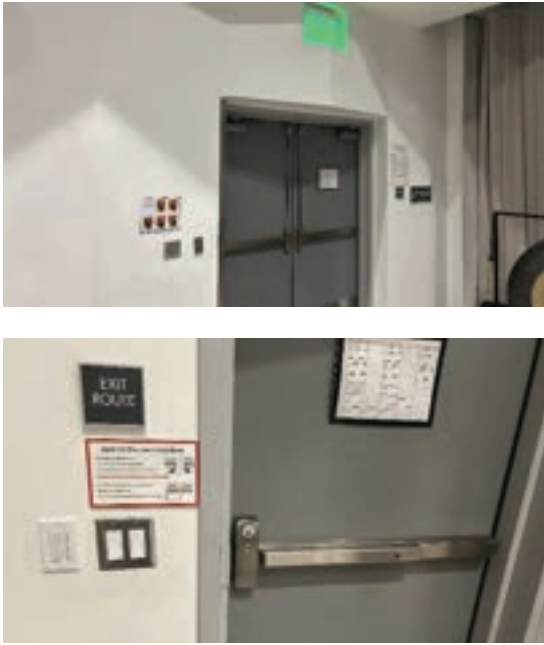
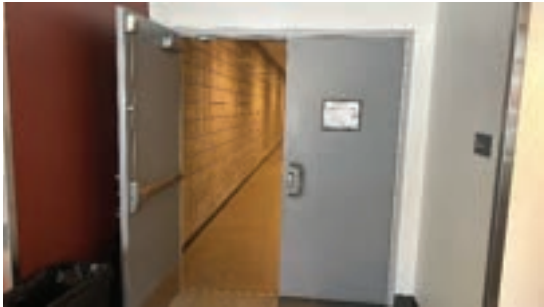

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
7	 	<p>The door at opening 123 is unlocked daily, the interior panic bar can be dogged, and the public side lever unlocked. This has potential risk as the lever and the panic bar could both be left in an unlocked state causing extra effort to secure in a lockdown as both sides of the door require locking. These doors have no electrification that would support immediate lockdown and lock/unlock on schedule if controlled by the access control system.</p>	<p>Remove the dogging feature and replace the panic bar key cylinder with a blanking plate. These doors should be electrified to support immediate locking upon lockdown activation and allow for remote locking/unlock.</p>	4
8	 	<p>Practice Rm. 124 has a sticker underneath the deadbolt key cylinder indicating that the door should remain locked when unoccupied. The door was found in an unlocked and open state. There is a throw on the interior that allows for the door to be locked from the interior. There is no door closer installed that would support positive latching and closure at all times. The side window panel has no window treatment applied allowing opportunity to eliminate visibility from the corridor in the event of a lockdown. Practice Rm's without the instruction displayed reference</p>	<p>Review door hardware installed and ensure that the ability to lock the door from the interior is available when occupied. Apply window treatments to restrict visibility from the corridor inwards.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>remaining locked, have had their internal throws removed. This presents risk as occupants are unable to secure doors if a lockdown occurs.</p>		
9		<p>The inner outdoor courtyard doors have panic hardware on the interior of the openings, these are dogged providing free egress at all times. Phone numbers applied to the openings on the exterior are small in text size and suggest that persons have been locked in this area. This was confirmed by faculty as an occurrence at one time. The doors are locked at the end of each day to eliminate opportunity for scaling of the courtyard wall and unauthorized entry occurring. Video surveillance is not installed monitoring activity.</p>	<p>Confirmed that doors are locked and unlocked on schedule. Install video surveillance to monitor activity after-hours, monitor the top of the courtyard wall for unauthorized scaling. Design text and finishes on signs for clarity and ease of reading.</p>	1
10		<p>Double doors at the rear entry #140 can be accessed via presenting a security credential at the HID card reader. There is signage installed on the door that indicates that brass key should not be used to enter and to use a security key card only. Signage also advises all UPS and FedEx deliveries that they must go to the front entrance. There is no means to communicate with the reception desk from this point and the signage is minimal in size, making it difficult for delivery drivers to easily read the instruction. Faculty have concerns with these doors as</p>	<p>Install a video intercom providing communication directly with the main entry desk. Interface access control and video surveillance systems to provide camera call-up triggered by door held and door forced alarm events. Install interior signage indicating that doors must remain closed and locked at all times.</p>	4

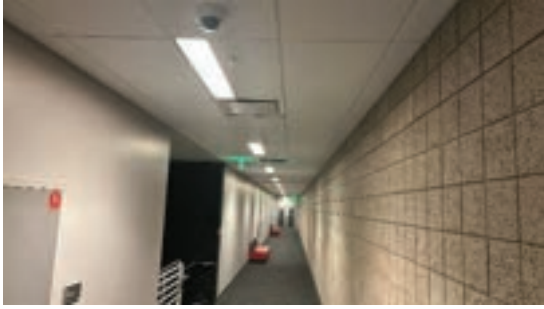



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>they have found them propped on several occasions without notification which allows unauthorized entry. A video surveillance camera mounted directly above the opening provides visibility of activity. Exterior video surveillance cameras are equipped with sun caps which are intended to negate glare.</p>		
11		<p>Video surveillance is not installed at this location to provide visibility of activity at the lockers and within the corridor.</p>	<p>Install video surveillance to monitor activity, consider a multi-sensor at the top of the stairwell landing to provide full 360 coverage of activity within and approaching the corridor.</p>	3
12		<p>Level one restrooms are equipped with deadbolt throws. The throws are unable to be used to throw the deadbolt from the interior to secure the door, the throw will allow a single retraction of the deadbolt to allow free egress if locked from the exterior. There is no public address system that provides opportunity for local communication if the building has been placed into a lockdown or shelter-in-place state.</p>	<p>Consider installation of public address speakers in all restrooms that can be placed into remote lockdown, to provide communication when this occurs and occupants to shelter-in-place. Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions.</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
13		<p>Soundproof practice rooms do not provide the opportunity for student occupants to secure the door from the interior in the event of a lockdown. Doors can be locked from the interior by brass key holders only, if locked from the interior, there are no telephones provided within learning areas that allow for communication to be made. All classrooms and practice rooms are reliant upon cell phone usage for communication.</p>	<p>Review the door hardware installed and consider replacing with internal lockable hardware. Provide telephones to support ability to communicate outwardly of needed during an emergency situation. Cell coverage was spotty during the assessment and reliance upon personal cell phones for communication is not recommended.</p>	4
14		<p>The Telecom Rm. Is not controlled by access control and is on a dedicated IDF/Data Rm., keyway that is restricted distribution. The room is climate controlled with a HVAC unit, there is no drip tray installed below the unit. The video surveillance cameras terminate within this room on patch panels connected to switches in the data rack. An America Dynamics network video recorder is located within the data rack, Cat 6 yellow cable is used for video cameras, and all were labelled with machine generated labels. The Software House access control head-end panels are wall mounted (cabinets were locked so inspection of hardware was not possible). 120V power to the Software House cabinet is provided by a quad receptacle rather than being hardwired to avoid potential tampering. The DMP intrusion detection enclosure houses the intrusion panel and the power transformer. The</p>	<p>All critical infrastructure rooms should be controlled entry via the access control system, providing an audit trace of persons who accessed or attempted to access such spaces. Develop Division 28 design standards that identify and document best practice installation including hardwiring main power supply to dedicated circuits rather than plugging power cables into receptacles that can be tampered with. Video surveillance should provide visibility of approach activity and activity within critical infrastructure rooms.</p>	3


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>back-up battery is dated as installed in 2021. There is no video surveillance camera installed within the room.</p>		
15		<p>Reference observation #6, this stairwell from level two down to level one allows access into areas behind doors leading from the lobby when closed and locked.</p>	<p>Reference recommendation #6.</p>	4
16		<p>No video surveillance camera in the corridor monitoring activity.</p>	<p>Install video surveillance to provide ability to monitor general activity in public corridor space. Use of multi-sensor or dual head cameras will provide enhanced visibility using the same infrastructure that would be required for a single fixed-dome camera.</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
17		<p>Double doors are electrified, with a key switch installed that applies power to retract the vertical rods to unlock the doors when activated. The doors are not monitored on any security system and Faculty were uncertain of why these doors were electrified, with understanding that the Fire Marshal drove it. The single opening can be opened from the exterior, but the trim can only be unlocked from the interior. The exterior function of the hardware is storeroom. The lock blok has been removed from the door.</p>	<p>General observation only. The purpose of electrifying these doors is unknown. Placing the doors into an unlocked state from the interior is not recommended if the doors are for egress purposes only.</p>	1
18		<p>Mechanical doors at the lobby leading into the corridors were observed propped open. There is no ability to automatically secure these doors as they are not held open on electrified hold openers, and the door hardware is not electrified. Faculty requested that they would like these doors and the single door on the other side of the lobby to be electrified to support immediate lockdown capability.</p>	<p>Apply access control measures to the doors to restrict access into the corridor space to authorized personnel and students only. Install video surveillance within the corridor to monitor general corridor activity.</p>	4
19		<p>Hardware applied to these restrooms on the second level is different to that on the first floor. Hardware is pull trim only and the doors cannot be locked from the public side. There is no video surveillance camera installed monitoring activity in this alcove which is setback from the corridor.</p>	<p>Install video surveillance to monitor activity outside of the restroom area. Internal public address is recommended to provide notification of emergency events such as lockdown to occupants of the restrooms.</p>	3





ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
20		<p>Extron screens connected to the AV system, all district computers, and laptops, receive the RAVE Alert notifications when they occur in addition to cell phones. Capability to secure the classroom door from the interior requires a brass key. In the event of a lockdown sheltering against the wall provides complete restriction of visibility for a person in the corridor attempting to identify targets.</p>	<p>Review the door hardware functionality installed, it is recommended that use of a brass key to secure doors be avoided, and internal thumb-turns be installed removing potential risk of fine motor skill failure in high stress situations. Additionally, a thumb-turn allows others to also secure the opening if the key holder becomes incapacitated or cannot locate the key etc.</p>	4
21		<p>Classroom door was observed propped open when a class was in session. Wedging of doors should not be permitted as it requires entering the corridor to successfully remove the wedge and then close and secure the door in a lockdown, this may place an occupant of the room in immediate danger.</p>	<p>Remove door wedges and consider a protocol that does not permit classroom doors to be propped open. Propping of doors may cause delay in efficiently locking and securing doors in a lockdown or emergency event. A standard operational protocol for the building is suggested.</p>	4
22		<p>The recording studio houses expensive equipment and is accessible via brass key. There is no monitoring of who enters the space or ability to monitor door status. A lack of district security standards fails to provide governance and minimum application of security measures. High value equipment rooms would typically be slated to receive access control measures i.e., card reader and electrified hardware.</p>	<p>Install access control measures to the opening to provide an audit trail of access and to support ability to monitor the door status with alarm events received if the door is forced or held beyond preprogrammed parameters. Video surveillance installed within the corridor should be programmed through systems interface to call-up on alarm event trigger.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
23		<p>Camera monitors activity at the stairwell, there are no additional video surveillance cameras in the corridor monitoring activity at the other end of the corridor.</p>	<p>Install video surveillance to provide ability to monitor general activity in public corridor space. Use of multi-sensor or dual head cameras will provide enhanced visibility using the same infrastructure that would be required for a single fixed-dome camera.</p>	3
24		<p>Faculty requested that a monitor be added to the staff break room wall that displays the buildings video surveillance video stream. Intent is not to spend time sitting watching cameras, but to have ability to glance and if something appears out of the ordinary activate a proactive response rather than react to incidents. No Faculty have access to the video surveillance system, and they are uncertain of who has viewing access, length of video retention, and approved use.</p>	<p>Install a wall mount monitor that streams live video surveillance feed from the building system. General activity awarenesses may provide valuable time to respond to something that seems out of the ordinary with appropriate response protocols proactively rather than responding reactively. The monitor is not intended to encourage "sit-and-stare" activity but support wider visibility and ownership of day-to-day security management.</p>	3
25		<p>Reference observation #8, regarding removal of internal throws to secure the practice room doors on the second level.</p>	<p>Reference recommendation #8.</p>	3
26		<p>The sidewalk adjacent to the main entry of the building has concrete blocks that serve as bollards to restrict vehicles from potentially traversing up onto the sidewalk. These are well spaced to restrict vehicles from also passing through. There are spaces at each end of the sidewalk that do not have concrete blocks deployed and vehicles could easily enter the sidewalk (there have been</p>	<p>Install additional concrete blocks to eliminate the vulnerability identified. If permanent blocks present accessibility issues for first responders or others, review alternate options including removal bollards. The ability for vehicles to access and park on the sidewalk should be eliminated (unless authorized).</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>instances of vehicles parking on the sidewalk). The concrete blocks are softened in appearance with low level landscaping within the CPTED recommended ground covering height of below 2' which is excellent.</p>		
27		<p>Signage on the exterior of the parking garage provides clear direction regarding parking permits and bays that can be used. The parking garage is locked at 10:00 PM each evening and a metal roller gate closes the main entry; free egress is maintained. Video surveillance is not installed to specifically monitor traffic entering and exiting the structure.</p>	<p>Install video surveillance to monitor incoming and departing vehicles. Use of license plate recognition (LPR) cameras would support identification of vehicles not permitted to park at the facility and or identify vehicle users with other issues that may require intervention by the parking office.</p>	2

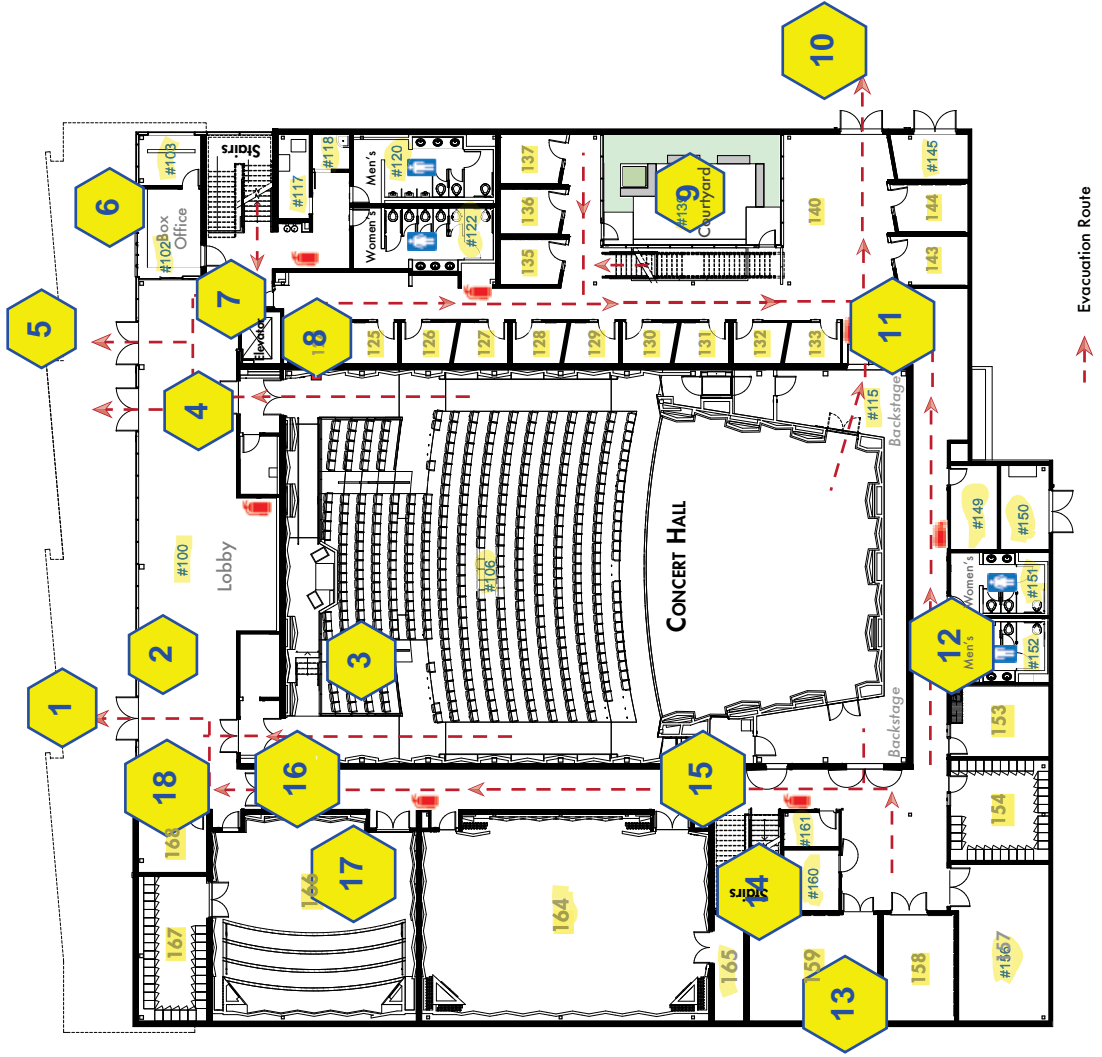
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
28		<p>Inconsistency in height of fencing installed on level one of the parking garage allows opportunity for unauthorized scaling of the fence to enter the parking garage. The fence adjacent reaches the ceiling of level one, the gap as shown in the image provides ease of access. Faculty shared concerns regarding this vulnerability and are aware of several students who have made it known that they climb the fencing to gain entry after the garage is closed.</p>	<p>Install fencing that eliminates the identified gaps in perimeter fencing on level one of the parking garage. Ability for scaling and unauthorized entry to the parking garage when closed should be mitigated as best possible. Fencing should be installed from the ground to the ceiling (deck of level two).</p>	3
29		<p>RCCD Police Department Parking Services Office located on level one of the parking garage has a monitor that provides visibility of all video surveillance cameras installed at the District Office, Coil Center, and the Culinary Arts Academy. Camera field of views appeared clear with exception of one camera that requires maintenance review to clean the lens to provide a clear field of view. There appeared to be cameras installed within classroom areas which is not consistent with camera deployment across the RCC campus.</p>	<p>Expand the ability for video surveillance to be monitored beyond this central point. Refer to individual site assessment reports with recommendations of local monitoring to support proactive response to abnormal behaviors observed. Review the cameras that provide visibility of class in session. Review with district legal counsel appropriateness of monitoring students unknowingly who are attending class.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
30		<p>Signage installed on pillars clearly identifies faculty parking spaces defined by yellow bays. As with RCC campus all faculty parking bays are yellow and public/visitors bays white. There is no signage either physical or painted on the tarmac that provides speed limit control. Emergency Phone Code Blue towers are located consistently in the same location on every level. All towers are consistent and use the Code Blue call stations.</p>	<p>Install signage that indicates the approved speed limit within the parking garage. Fixed and tarmac signage is recommended.</p>	2
31		<p>The perimeter wall on the top deck of the parking garage is approx. 4' in height. There have been suicides occur at the RCC parking garage and the top deck measures in place do not provide any potential restrictions to stop suicides by jumping from occurring. The elevator landing sliding door on each level is glass, this is</p>	<p>Replace signage that is sun-bleached with new. Install video surveillance throughout the parking garage providing visibility of activity. Replace the glass elevator landing doors with more robust steel material, if visibility from within the cab is the desired intent consider doors that are a combination of steel (lower) and glass (upper) to reduce damage</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
	   	<p>unusual for this type of built environment setting. We were advised that the glass doors have required replacing causing negative operational impact on facility use and also causing expensive repair costs. Signage reference the use of the garage is displayed at each stairwell, signage that is exposed to direct sunlight for extensive periods of the day requires replacement as the text is difficult to read.</p>	<p>impact on operations dysfunction and continual increases in operating costs.</p>	<p style="background-color: yellow;">High</p>

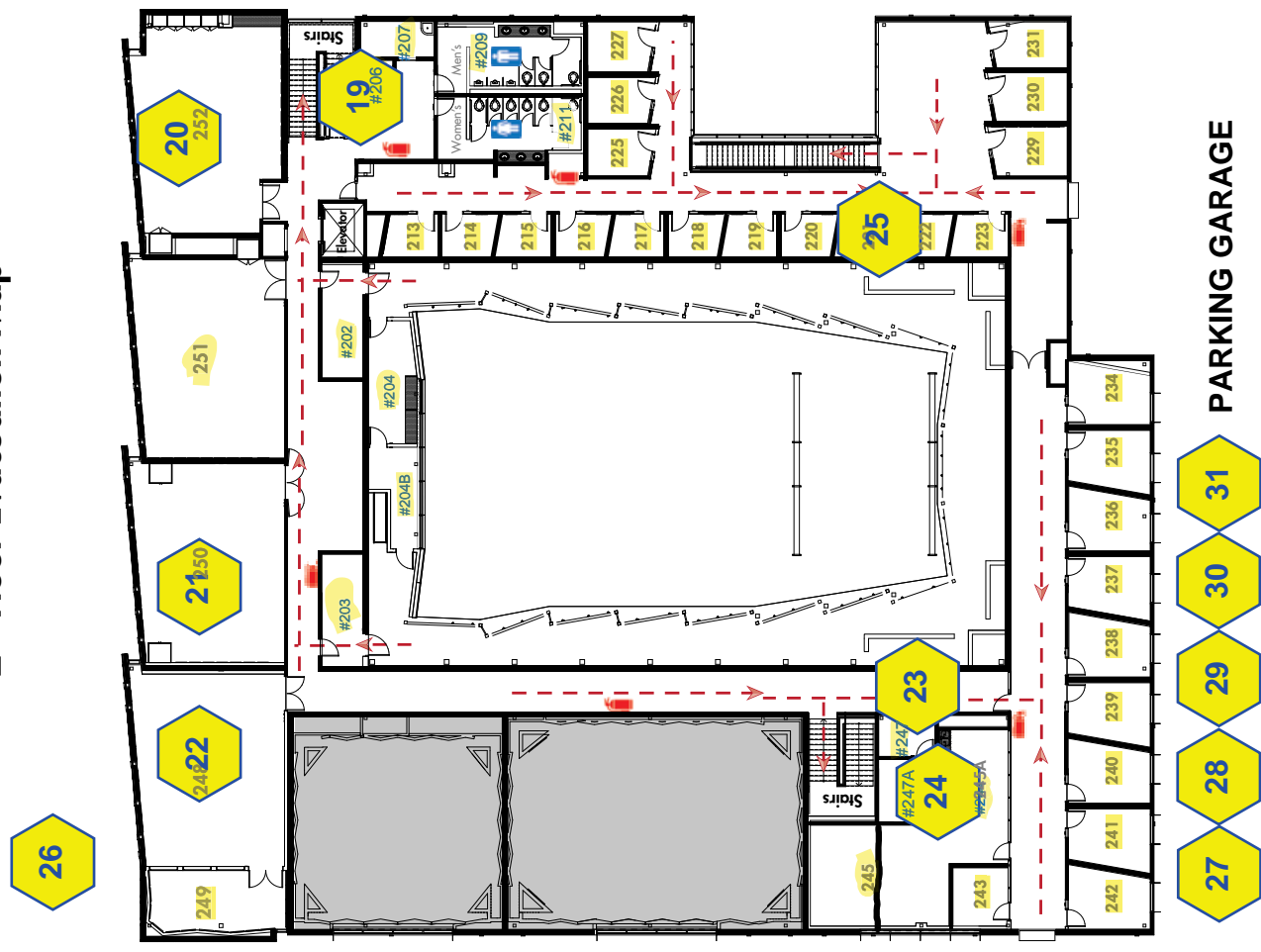
**HENRY W. COIL SR & ALICE EDNA COIL
SCHOOL FOR THE ARTS**

1st Floor Evacuation Map



**HENRY W. COIL SR & ALICE EDNA COIL
SCHOOL FOR THE ARTS**

2nd Floor Evacuation Map



Moreno Valley College

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>Dental Center Building B external video surveillance camera appears to have been removed and never replaced. Cable remains and should be removed if no intent to reinstate a camera. Exterior doors are all controlled with access control measures with electrified lock sets and door position monitoring contacts. The doors are not unlocked on schedule and require presentation of a valid security credential to unlock. The gas utility mains can easily be tampered with as there is no protective cage. Exterior LED lighting is located on the wall along the exterior of the building.</p>	<p>Review code and AHJ requirements, if approved install protective caging over utility mains, breakaway locks must be installed to support first responder access and be compliant with NFPA guidelines. Install a video surveillance camera at the location where the cable remains, replace cable with new.</p>	1
2		<p>Fixed bollards restrict vehicle access to the rear of Building B. There is no fixed signage within the parking lot that clearly indicates student and faculty parking areas. Lighting is minimal in its distribution within this parking lot.</p>	<p>Install additional signage that clearly identifies parking bays for staff and parking bays for students. Refresh paint markings to mirror the signage communication. Ensure all site signage is durable against human tampering and natural weather events. Design text and finishes on signs for clarity and ease of reading. Install additional lighting to mitigate areas of darkness and shadows within the parking lot.</p>	2
3		<p>Lighting in the parking lot is LED downwards facing luminaire, the lighting application is appropriate however, the adjacent tree is covering the lighting fixture potentially impacting light distribution. The access road entry swing arm gates are closed daily restricting access to parking lots outside of college hours.</p>	<p>Prioritize maintenance and repair that could affect the security of facilities such as perimeter fencing, lighting, facility locks, and access points.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
4		<p>The emergency call box has a campus map that does not have a legend to clearly identify the location of the call box placement. The call box speakers are used to provide public address announcements. There is no video surveillance camera monitoring the emergency call box providing the ability for camera call-up providing real-time visibility when a call is placed.</p>	<p>Consider use of a standard Code Blue all-in-one call station with blue strobe unit in the future. Use the Code Blue towers to support video surveillance cameras, solar back-up, and other devices as appropriate. Interface the Code Blue call stations with other security electronics systems providing camera call-up and notification when a call is activated. The provision of a map illustrating the location of the emergency tower is a good measure that should be considered for use across district emergency towers.</p>	4
5		<p>Seating area provides natural surveillance and ability to get eyes on activity when occupied. The restrooms for staff are controlled entry via security credential. The student/public restrooms are unlocked on schedule with no access control card readers, but electrified strikes installed. There is no communication ability with restroom occupants if the electric strikes are placed into lockdown. There have been instances of youths scaling the roof, there is no video surveillance installed that would support forensic review.</p>	<p>Install external video surveillance monitoring the restroom areas, the public restrooms were unlocked during the evening and available for unrestricted use and potential sleeping within by homeless. Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. Ability to notify restroom occupants when an emergency event or lockdown has been activated is important. Install a public address system(s) that can verbally advise building occupants of the appropriate</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			action (e.g., evacuate, shelter-in-place) to take in any event.	
6		<p>Access control is heavily deployed in the dental buildings. The ability to secure all the access-controlled openings from the main reception lobby area can be achieved, by activation of the emergency door lock mushroom buttons that are installed on the walls. An access control credential is required to arm and disarm the intrusion system. There is no video surveillance monitoring lobby activity.</p>	<p>Install a lockdown button at the reception desk eliminating the risk of potential interaction with bad actors by staff if they have to lockdown a building by activating the wall mount push buttons. Convenience of a desk mount push button may provide valuable seconds to the lockdown activation response. Install a multi-sensor video surveillance camera in the reception lobby area to monitor general activity.</p>	4
7		<p>A local public address system is installed across the three dental buildings. Communication can be made from the main reception desk using a desk mount microphone. Interior access control doors do not have door position monitoring contacts and the electrified hardware simply locks/unlocks without indicating the door status. There is no ability to monitor the position of the doors i.e., door forced/held. A lockdown of the dental department buildings cannot currently be made directly at the lobby desk.</p>	<p>The local public address system is excellent but local only and does not include the restrooms identified in observation #5. Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. Ability to notify restroom occupants when an emergency event or lockdown has been activated is important. Install a public address system(s) that can verbally advise building occupants of the appropriate action (e.g., evacuate, shelter-in-</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>place) to take in any event. Develop security design standards that mandate that all access-controlled openings are monitored for status by door position monitoring contacts. Application of access control without ability to know door status renders the system and expensive electrified brass key.</p>	
8		<p>Classroom 105 at the dental center is accessed via security credential. The door can be placed into an unlocked state by presentation of the credential twice at the reader and relocked by presenting the same credential a further two times. An emergency door locking button was located within the space. The door hardware cannot be dogged as a blanking plate is installed removing potential to retract the latch in an unlocked state. A lock blok had been removed. The room/building is monitored on the intrusion detection system, with internal motion sensors and door position monitoring contacts. The entire dental department buildings intrusion system is armed and disarmed centrally at the main building arming station. There were no window treatments provided. Operational expectation of all classroom doors is that they remain closed and locked at all times including when lock bloks are installed. Written protocol</p>	<p>Panic bar blanking plates at access-controlled openings with such hardware should be a standard approach at all access control panic hardware openings. The closed locked door policy is excellent and should be formalized by written policy. Review the implication of lock blok use at openings that remain in a locked state. There will be alarm event implications that require working through if future systems are interfaced i.e., access control and video surveillance, false door held alarms may be received. Window treatments should be installed to restrict visibility from the public side, consider ballistic film. Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>states that doors must remain closed and locked when class is session. Lock blocks maybe used for convenience of student entry and doors closed and locked when all students have arrived at class</p>		
9	   	<p>Emergency phone is not monitored or integrated with any video surveillance cameras. There is no video surveillance installed on the exterior of the dental buildings, monitoring general pedestrian and parking lot activity. The dumpster cage remains open and unlocked. There is no physical signage within the parking lot that clearly indicates student visitor or faculty parking spaces. Speed limit signage is also lacking at this area. There are posts that signage previously hung on still present without signage, lack of maintenance does not impart a positive first impression on campus visitors. The tarmac signage markings in the parking lot require refreshing. Maintenance activity should occur to eliminate the impression that safety and security is an afterthought.</p>	<p>Install video surveillance on the building perimeter to provide situational awareness and forensic viewing capability. Interface video surveillance with the emergency call phones. Provide wayfinding and directional signage indicating the location of the area on campus in relation to other buildings. Clearly define the parking bays and permitted use. Design standardized text and finishes on signs for clarity and ease of reading. Display building information at vehicle control points and provide site signage that is durable against human tampering and natural weather events. Post signage on the perimeter of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.).</p>	3

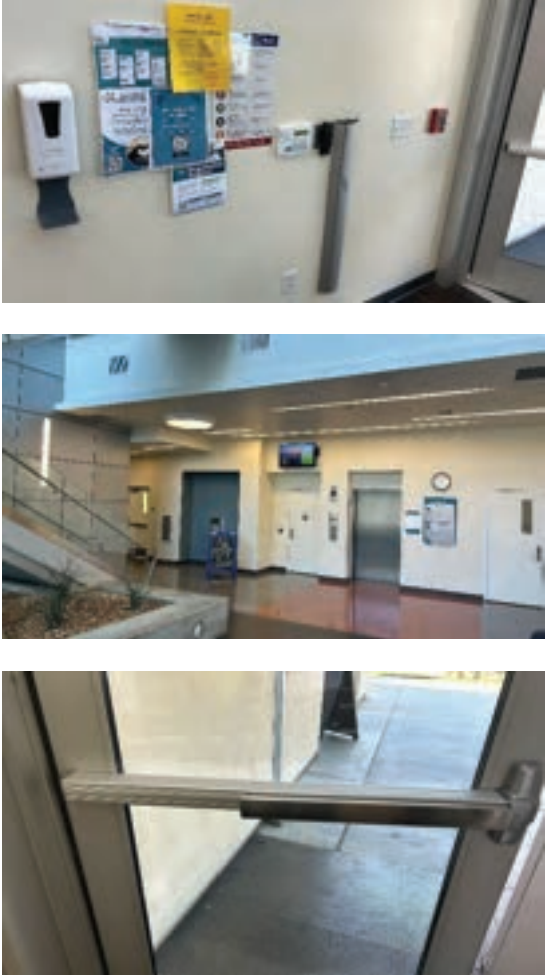

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
10	NOT USED			
11		<p>Rather than secure and compartmentalize each parking lot, vehicle controls are installed at entryways from public and campus roads. Swing-arm barriers are assumed to be closed each evening by the campus police and secured with chain and padlocks.</p>	<p>Post signage on the perimeter of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.). Review the memorandum of understanding with campus police and identify tasks and responsibilities, the gates appear not to be closed and locked at night.</p>	2
12		<p>Signage indicating the main entry point onto campus is installed off of College Drive. Fixed signage installed adjacent to the sidewalk provides directions regarding parking permits etc. Some of the signage appears to be weathered and in need of replacement. Speed limit signage indicating 15 mile per hour speed restriction is not consistently displayed across campus.</p>	<p>Replace signage that is sun bleached. Ensure all site signage is durable against human tampering and natural weather events. Install consistent speed limit signage throughout the campus. Consider installation of speed cushions at this location and other select locations across campus to restrict and maintain speed control.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
13		<p>The main vehicle entry point into the college has no vehicle monitoring capability with no license plate readers installed. There are several issues with the main point of vehicle entry, specifically the lack of bollards at the bus drop off area which provides completely unrestricted vehicle access towards the Technology Building. The ADA drop off/pick up point is not separated from the bus drop off area which presents risk. There is no emergency telephone installed in this prominent foot traffic and vehicle area. Seating is available to provide natural surveillance and encourage eyes on activity. The tree canopies are above 6' which is excellent and provides unrestricted visibility of activity.</p>	<p>Install removable bollards adjacent to the bus stop to mitigate against potential unrestricted vehicle access. Reference recommendation #12 regarding speed control suggestions. Consider installation of a Code Blue emergency phone tower at this location which encounters heavy foot-traffic. If future intent to expand video surveillance is an intent, this location is ideal for use of license plate reader cameras as the bulk of campus traffic enters at this juncture.</p>	3
14		<p>Administration parking spaces are identified with physical signage and white painted parking bays. This is inconsistent with the other directions across campus with faculty and staff parking identified with yellow parking bays. ADA parking is not provided in all parking lots. There is no video surveillance monitoring the emergency</p>	<p>Recommend that a district standard be applied regarding the coloring of parking bays for staff and student use. A consistent approach promotes familiarity, culture, and expectation of a RCCD campus environment for users. Consider video surveillance coverage in parking lots to monitor general activity, develop a security</p>	2





ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>phone or general parking lot activity.</p>	<p>design standard that promotes a consistent approach.</p>	
15		<p>Access to the service road around the entire campus is easily achieved as there are no barriers restricting access. If the campus access road swing arm barriers are not closed as presumed occurs daily, free vehicle access is maintained after normal hours. There is no video surveillance monitoring of the service lane activity.</p>	<p>Reference recommendation #11 regarding the campus police MOU and securing of swing arm barriers/gates. Consider installation of removable bollards to restrict access to authorized vehicles with keys provided in a Knox box. If mechanical bollards are impractical due to deliveries etc., consider an electrified access-controlled swing arm barrier. Intent is to restrict unauthorized vehicle access. Video surveillance should be installed to monitor general activity.</p>	2
16		<p>Access to the library from the service road provides unrestricted pedestrian entry as the exterior door opens upon activation of the exterior motion sensor. The exterior overhang provides an area for homeless to sleep etc., there is no video surveillance of activity at the under hang or of encroachment from the adjacent land. There appears to be no operational need for this door to be unlocked and provide access at this opening.</p>	<p>Install video surveillance to monitor general area activity, a multi-sensor camera would capture extensive area activity. Review the operational intent of the opening, are there any code requirements requiring the door remain open to the public side at all times? If no, remove the exterior opening feature and allow free egress only. This door was operational at 9:30 PM and provides ease of ingress without observation to anyone.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
17		<p>The landscaping adjacent to the Student Academic Services (SAS) building provides potential areas of concealment as the foliage is above the CPTED recommendation of 2'.</p>	<p>Perform periodic landscaping maintenance to reduce ground covering overgrowth and areas of concealment. Utilize CPTED best practices.</p>	2
18	  	<p>The SAS building interior common seating area is effectively a goldfish bowl with unrestricted visibility from the exterior public side in. Access to the space is managed via scheduled unlock and lock of access control openings. The single Sony fixed field of view cameras are no longer available as Sony no longer manufacture the product. The wall mount emergency call station instructional print is weathered and in need of refresh. The stairwell exit door is identified with signage on the frame header, this is not legible from a distance as the print is small and not bold. The door has no key cylinder providing access from the exterior. First responders are unable to enter without force, there is no Knox Box located adjacent to the access points containing keys and access credentials.</p>	<p>Review programming and power at all emergency call stations with strobes, strobes should be illuminated at all times to draw attention to their location. This is a best practice approach that should be a district standard. Replace all sun-bleached signage with new, ensure all site signage is durable against human tampering and natural weather events. Apply door numbering that reflects emergency evacuation plans, use text, and finishes on signs that provide clarity and ease of reading. Refer to the Fire Marshal regarding accessibility to the stairwell exit door. Window treatments should be installed to restrict visibility from the public side, consider ballistic film. Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment.</p>	4


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
19		<p>The free speech area at the corner of the SAS building lacks video surveillance monitoring activity across the area. There is no emergency code blue tower in this area that provides ability to make emergency calls from the area that can be heavily populated. Natural surveillance and eyes on activity is supported by the placement of seating areas used by students. Landscaping is well maintained; however, the rosebushes are below 6' and above 2' obscuring direct visibility across free speech area.</p>	<p>Consider installation of a Code Blue emergency phone tower at this location which encounters heavy foot-traffic. Use the emergency tower for deployment of a multi-sensor camera providing visibility of activity at the phone and surroundings. Monitor the growth of the rosebushes, eyes-on-activity visibility should not be impaired.</p>	2
20		<p>Exterior of the main entry to the SAS building has a wall mount emergency call station and single fixed field of view camera. A PTZ camera is viewing straight out into the free speech area, there appears to be a power issue with the camera with a constant buzzing heard. Access into the building after hours can be achieved by presentation of a valid security credential. There are two exterior card readers adjacent to the ADA push plate, there is uncertainty on why two readers are present. A rock is placed outside of the door which clearly indicates that is used for propping of the door. Disarming/arming of the</p>	<p>Review programming and power at all emergency call stations with strobes, strobes should be illuminated at all times to draw attention to their location. This is a best practice approach that should be a district standard. Review the PTZ power issue and verify if the camera is operational, replacement with a multi-sensor camera would enhance video field of view. Review the automatic operated opening and ensure that the door sits in the frame flush. All rocks and other items potentially used to prop doors should be removed.</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>intrusion system uses a security card reader adjacent to the DMP keypad. There is no video surveillance within the internal lobby area. The single main entry door does not fully close and latch upon closure. Review of the automatic door operator should occur. A Knox Box is installed on the exterior of the entrance. An emergency procedure chart is installed in the lobby area, these are installed typical across all classrooms.</p>		
21		<p>Several fixed field of view video surveillance cameras are installed on the exterior of the south side of the SAS building. Cameras are installed consistently on each exterior level of the bridges leading from the Humanity Building. Replacement of these single field of view cameras with multi-sensor cameras would provide a significant increase of general camera coverage using existing cable and infrastructure.</p>	<p>Recommend replacement of cameras with newer dual head or multi-sensor cameras as part of a refresh program. The cameras currently are sufficed for monitoring of activity.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
22	 <p>The first photo shows a building entrance with a glass door and a concrete pillar. The second photo shows an outdoor walkway with palm trees and a building in the background. The third photo shows an indoor stairwell area with a concrete pillar and a blue sign.</p>	<p>Placement of video surveillance cameras is well intended; however new technologies have now provided ability to monitor significantly increased areas using a single multisensor camera with several lenses. Mounting of a camera at the stairwell would provide coverage of activity at the SAS building entry, Humanities building entry, and approach to the stairwell.</p>	<p>Install a multi-sensor camera providing four individual fixed fields of view from one housing and cable. Interface cameras with access control openings, as necessary.</p>	2
23	 <p>The first photo shows an outdoor area with a large overhead canopy structure and a paved walkway. The second photo is a close-up of a circular ground porthole in a concrete slab.</p>	<p>An overhead canopy system supports AV equipment that is mounted on the frame. This is expensive equipment with no video surveillance applied monitoring general activity. Expensive spotlights installed into ground portholes have experienced vandalism.</p>	<p>Install a video surveillance camera to monitor activity providing situational awareness, forensic review, and to serve as a deterrent to vandalism.</p>	1


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
24	  	<p>Vehicle access to the rear of the SAS building is unrestricted. The emergency call station identification number is weathered, and the unit number cannot be easily identified. There is inconsistency in deployment of maps at call stations to help call users identify their location. Signage above doors is inconsistent in the size and font of text used, it is difficult to read from a distance. Video surveillance lacks consistency in application and edge device type installed.</p>	<p>Reference recommendation #15 regarding installation of vehicle barriers. Review programming and power at all emergency call stations with strobes, strobes should be illuminated at all times to draw attention to their location. This is a best practice approach that should be a district standard. Replace all sun-bleached signage with new, ensure all site signage is durable against human tampering and natural weather events. Apply door numbering that reflects emergency evacuation plans, use text, and finishes on signs that provide clarity and ease of reading.</p>	2
25		<p>The Humanities building is adjacent to an open space area which provides visibility into the building from a vantage point. There is no ballistic film applied to the existing glazing, and concerns were raised by occupants during a recent lockdown that visibility and exposure is concerning. There</p>	<p>Window treatments should be installed to restrict visibility from the public side, consider ballistic film. Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>are issues with protocols being followed as experienced in the recent lockdown drill with shelter in place instruction ignored by some participants.</p>	<p>site risk assessment. Create formalized policy and procedure regarding lockdowns and shelter-in-place, distribute and provide training for staff, students, faculty, and other campus users.</p>	
26		<p>The main entry into the Humanities building has no access control measures applied to it and there is no video surveillance monitoring general activity. There is no signage that clearly indicates our celebrates that this is the main access point into the building. The landscaping is excellent providing natural territorial reinforcement, with a good setback between pedestrian access space and the building perimeter. Glazing is treated with film reducing glare from the sun. There is no ballistic film applied to any of the glazing.</p>	<p>Reference recommendation #25 regarding glazing treatment. Install video surveillance to monitor general activity. Install signage that clearly defines the building function and drives users to the main entry point.</p>	3
27		<p>Second level rear entry to the Humanities building is not access controlled and free ingress is provided whenever the door is unlocked. There is no video surveillance on the interior or exterior and there is a stairwell that provides a potential area of concealment. There have been consistent</p>	<p>Install interior and exterior video surveillance cameras, consider controlling the door on the access control system to allow remote lock and unlock capability. Review and consider addition of vape detectors that terminate to the security electronics system, active monitoring of the system</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>issues of vaping occurring in the restrooms with the smoke alarms triggering and response required by the Fire Dept'. There are no dedicated vape detection units that are terminated to the access control system. The lack of video surveillance cameras fails to provide ability to forensically review and identify persons entering and exiting the restrooms at the time of vape detection.</p>	<p>required to support response protocols (require developing).</p>	
28		<p>Example of potential unrestricted vehicle access adjacent to the Humanities building. HVAC equipment is secured behind chain-link fencing and gates. There is no video surveillance on the exterior of the Humanities building, providing situational awareness and forensic viewing capability of activity. Video surveillance camera installation across campus is sporadic in its placement with many areas that have zero coverage.</p>	<p>Reference recommendation #15 regarding installation of vehicle barriers. Install video surveillance.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
29		<p>ADA parking spaces at the upper parking lot adjacent to the portable classrooms are marked with paint signage on the tarmac and physical signage. There is an emergency code blue tower and LED cut off lighting adjacent to the ADA access path. There is no video surveillance installed. Lighting luminaires are down cut-off, some luminaires are obstructed by tree canopies that are below them. This may impede the effectiveness of the lighting distribution.</p>	<p>Review programming and power at all emergency call stations with strobes, strobes should be illuminated at all times to draw attention to their location. This is a best practice approach that should be a district standard. Perform periodic landscaping maintenance to trim tree canopy overgrowth and areas of obstruction of lighting. Utilize CPTED best practices.</p>	4
30		<p>Access into the tarmac area at the portables is unrestricted with A-frame signage indicating that the road is closed. The A-frame signs serve no purpose if a vehicle were to consider entering the space they could easily move them. The swing arm barrier is open, should be closed, and locked to restrict vehicle access if this is intended.</p>	<p>Close and secure the swing arm barrier, A-frame signage can remain as a means of communicating that access is closed.</p>	2
31		<p>Portable classroom door remains in a locked state all times but can remain open using a lock blok. This ensures that positive latching occurs immediately upon retraction of the lock blok and door closure. An intrusion arming/disarming station was observed, this</p>	<p>Consider implementation of Everlux photoluminescent Evacuation Plans that hold ambient energy providing visibility in the event of a power outage and darkness. These are used at Norco College and should serve as the standard across all RCCD campus.</p>	1



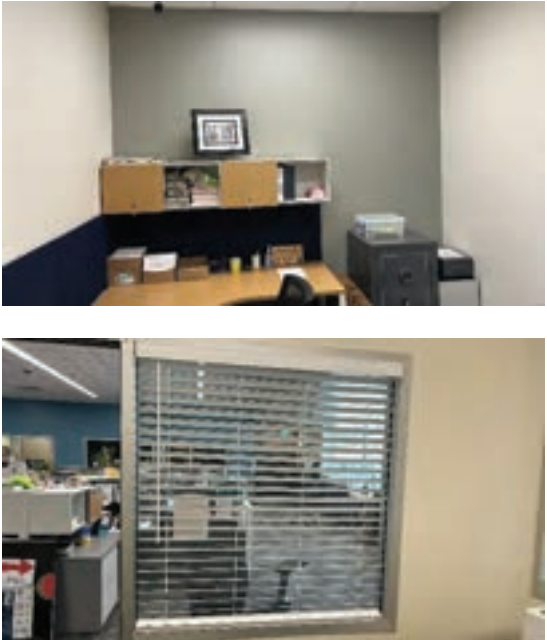
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>station arms all the monitored portables. New and legacy evacuation maps are present, legacy maps should be removed. Emergency procedures are installed as typical across campus.</p>		
32		<p>PSC Rm. #22 has interior locking door hardware via a thumb-turn lever, lock blok installed as typical. Window grill installed on the exterior serving as a deterrent to vandalism, there is no internal window treatment restricting visibility inwards. Evacuation map and emergency procedures are posted on the wall as typical.</p>	<p>Install window film that restricts visibility into the classroom from the exterior. Window treatments should be installed to restrict visibility from the public side, consider ballistic film. Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
33		<p>Restrooms at the PSC area are accessible via brass key only with the student and public restrooms unlocked manually on schedule. The internal deadbolt levers have been disabled these should be removed completely. There is no internal or external public address that provides communication if a lockdown has been activated. There is no emergency phone tower located in this area and zero video surveillance.</p>	<p>Consider installation of a Code Blue emergency phone tower at this location which encounters heavy foot-traffic. Use the emergency tower for deployment of a multi-sensor camera providing visibility of activity at the phone and surroundings. Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. Ability to notify restroom occupants when an emergency event or lockdown has been activated is important. Install a public address system(s) that can verbally advise building occupants of the appropriate action (e.g., evacuate, shelter-in-place) to take in any event.</p>	4
34		<p>Speed limit 5 MPH signage installed on the road adjacent to the PSC Evacuation Zone P space. This is a well-placed example of speed control signage; this is not reflective of signage across campus which is minimal related to speed. There are speed bumps located along the roadway intermittently serving as a physical measure to reduce vehicle speed.</p>	<p>Ensure all site signage is durable against human tampering and natural weather events. Install consistent speed limit signage throughout the campus, there is inconsistency in speed limits displayed across campus. Consider installation of speed cushions at this location and other select locations across campus to restrict and maintain speed control.</p>	2

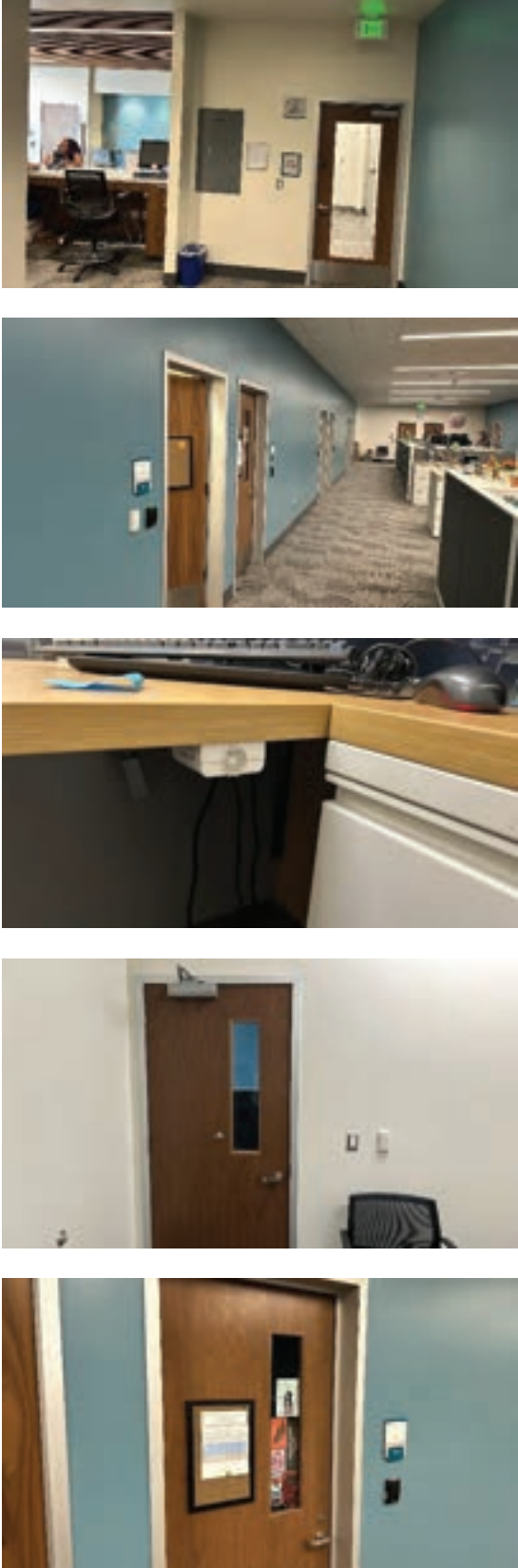
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
35		<p>Emergency call phone is located in an obscure location difficult to locate from the upper PSC buildings. There is zero video surveillance monitoring activity of general activity or when a call is placed at the call station.</p>	<p>Provide signage that directs campus users to the emergency phone location if needed. Use text and finishes on signs that provide clarity and ease of reading. Use the emergency tower for deployment of a multi-sensor camera providing visibility of activity at he the phone and surroundings.</p>	2
36		<p>The height of the ground coverings is above CPTED recommendation of 2' and provides an area of concealment for bad actors. Visibility form within the classrooms is minimal.</p>	<p>Perform periodic landscaping maintenance to reduce ground covering overgrowth and areas of concealment. Utilize CPTED best practices.</p>	2
37		<p>Access to the multiple purpose room (MPR) is using a brass key, there are no access control measures oat the building. It is monitored with intrusion detection. The rest and locker rooms are open for general public. Use, this presents risk as there been instances of homeless persons using these facilities without authorization. The facilities are also open to public use when the sports field are in use. The college allows use of their facilities rather than provide porta-pottys for public convenience. There is no video surveillance in use monitoring general activity. The Facilities Dept. standalone Panasonic VMS does not capture the entry points of the MPR.</p>	<p>Install access control to support remote locking and unlocking of the facility; install video surveillance to the exterior monitoring general activity, and interface with controlled openings for alarm event camera call-up. Review operational needs and consider use of porta-pottys for public use mitigating college risk and liability of unrestricted access for use of facilities by the public.</p>	4


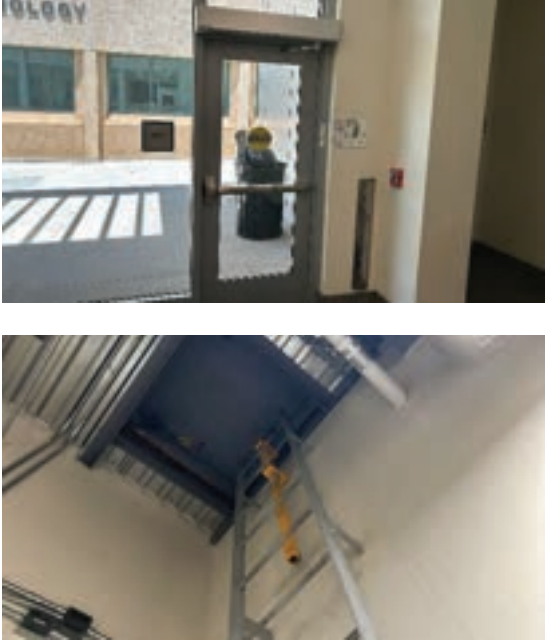
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
38		<p>Signage on the Welcome Center (WC) blends into the metal façade making it difficult to identify the building name. The pedestrian sidewalk is well defined and set back from the building with bollard lighting. Ground covering is above the 2' recommended CPTED landscape ground covering height but does not provide support of natural territorial reinforcement and access control.</p>	<p>Review the building identification signage, text size, style, color, and font should be consistent across campus to generate a sense of culture, belonging, and identity. The WC signage is non-descript and should be prominently identifiable by campus users.</p>	3
39		<p>The WC main entry sliding doors are controlled on the access control system with a card reader providing entry via security credential when doors are locked. The video surveillance camera mounted on the exterior of the entry is not focused on the main entry door.</p>	<p>Adjust the existing camera lens to capture activity at the exterior opening to the WC. Replace if needed with a dual-head camera with one lens fixed on the entry.</p>	1
40		<p>Main entry doors can be locked from the interior using the toggle switch mounted on the door frame. Video surveillance cameras are installed in the main atrium area monitoring general activity. The arming station for the intrusion system is armed and disarmed using the HID card reader. The video</p>	<p>Consider controlling the door on the access control system to allow remote lock and unlock capability. Window treatments should be installed to restrict visibility from the public side, consider ballistic film. Glass should be selected and designed in accordance with relevant standards to meet the security</p>	4




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>surveillance cameras are Sony Illustra. Window treatments are not applied to the lobby glazing.</p>	<p>requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment.</p>	
41		<p>Data Rm. 102 is accessible via security credential only. The door is equipped with a door closer ensuring positive latching upon closure, this should be a standard at all access control doors. Video surveillance camera monitors activity at the rack. An American Dynamics NVR is located within the room along with Software House and DMP enclosures. The room is climate controlled.</p>	<p>Conditions at this data room are typical of security best practices found at rooms with critical infrastructure. The measures in place should be formalized within security design standards.</p>	0

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
42		<p>Cashiers' office staff and back of house space is accessible via access control only. Video surveillance cameras are monitoring general transaction activity at the counter. There is a plastic screen along the counter that was installed during the pandemic that provides some means of barrier between public and the staff. There is no roller shutter to secure the space after hours. Panic buttons are momentary release installed ad hoc under the transaction desks.</p>	<p>Consider deployment of hardwired panic buttons at all transaction workstations. Recommend replacement of the plastic screen with fixed glazed transaction pass through windows per the cashiers' office. Provide a physical barrier between staff and public. At minimum, a roller grille should be installed to allow compartmentalization of the space and eliminate the open nature currently observed.</p>	3
43		<p>The office containing the safe at the cashier's office at the WC is accessible by access control only. The safe remains locked at all times; a video surveillance camera is installed monitoring general activity. At the time of assessment, a board with brass keys was found sitting on the top of the desk, brass keys should never be left out of a controlled enclosure. Window treatments have been applied to the interior of the office to restrict visibility in when monetary transaction activity occurs. The video surveillance camera should be integrated with the access control system to provide camera call up on</p>	<p>Integrate security electronics to support camera call-up on alarm event. Secure keys in a keyed enclosure with controlled key distribution.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		door held or door forced alarm events.		
44		<p>Specific office spaces within the cashier's office have been identified for use as areas of refuge during a lockdown. These office spaces require window treatments to be applied; here is a current work order awaiting completion regarding this issue. Exterior windows are equipped with blinds that restrict visibility from the exterior when lowered. The single exit door in the cashier's office provides free egress to the exterior and is encouraged to be used in the event of a need to evacuate.</p>	<p>Apply the same measures as applied to the office containing the safe. Ensure that VoIP telephones are installed in all offices identified as areas of refuge, radios should also be considered for use as in event of power failure and loss of network telephone communication. Conduct training that engages the single exit door as a means of exit in a lockdown etc., do not assume that occupants of the space naturally would consider the potential escape route.</p>	3
45		<p>The Counseling Office is equipped with a card reader for authorized entry only. This door is often held open using the lock block. There is risk to those who work within the space by providing free ingress as altercation with agitated persons is possible. There is a panic button located at the main transaction counter that communicates directly to Riverside Sheriff Dispatch. There is no video surveillance monitoring the corridor side of the entry. The inner counseling offices are all equipped with access control measures and</p>	<p>Provide remote release capability at the reception desk to provide controlled entry into the space through the access-controlled opening. Consider installation of strobes and ceiling Piezo sirens to provide visible and audible notification of panic alarm activation within the individual counselling offices. Operationally review the current practice of window vision panel coverings, consider protocol that restricts coverings to 75% or AHJ recommendation that provides privacy but ability for first responders to view in.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>panic alarms. Some counselors reduce visibility through the window vision panel into the room using makeshift covers. This is concerning as there could be a medical issue, request for assistance, or other situation occurring with no ability for responders and support staff to observe activity from the unsecured side. If a panic button is activated within the counseling offices, there is no annunciation either audibly or visually within the office atrium that indicates that support is required.</p>		

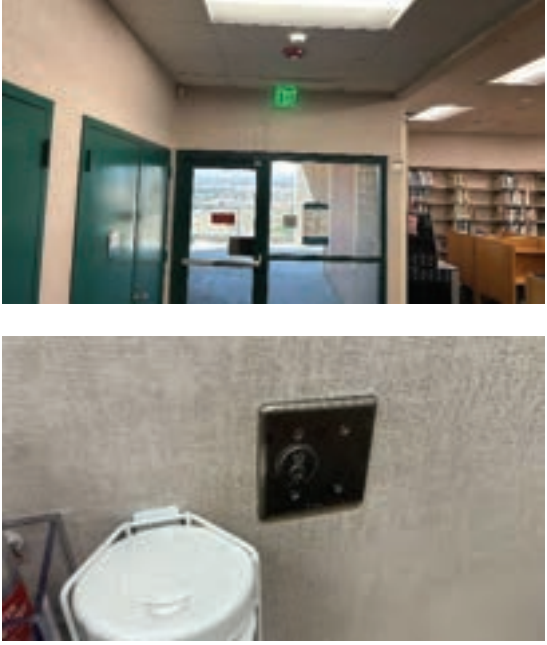


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
46		<p>The controlled corridor entry door leading into the student engagement center does not positively latch. There are exterior window treatments installed, but no window treatments on the corridor facing glazing or door. The card reader is installed in a location within the door swing, which is not best practice, as it could potentially result in the door hitting someone on exiting if a person is presenting a credential to access.</p>	<p>Conduct a maintenance review to correct the door operation ensuring that there is flush fit within the frame and positive latching upon closure. Security design standards should provide direction that card readers where possible are not installed within the door swing or on the hinge side. Window treatments should be installed to restrict visibility from the public side, consider ballistic film. Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment.</p>	4
47		<p>Exterior opening is dogged open remotely via the access control system. On activation of a lockdown the door latch is released. There is no video surveillance in the corridor monitoring activity at the entry and restroom setback entrances. There is a mix of Allegion and Corbin Russwin hardware in use across campus. The roof access within the controlled entry Janitor Rm. 162 does not appear to be secured with a padlock or monitored on either the intrusion or access control systems.</p>	<p>Install video surveillance to monitor corridor, exterior point of entry, and setback restroom approach. Develop security standards that include provision of video surveillance cameras at all building points of entry and interface with access control and intrusion detection systems for camera call-up on alarm event. Consider securing the roof hatch with a breakaway padlock and monitor position with a surface mount monitoring contact. As the security program evolves standardization on a single door hardware provider would provide consistency of product installed, streamline product management knowledge needs, and present a consistent feel and appearance across campus.</p>	2






ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
48		<p>The single stall restroom door hardware allows securing of the door from the interior, there is a privacy indicator notifying that the stall is in use.</p>	<p>General observation, this is a good example of appropriate hardware at this type of room function.</p>	0
49		<p>Break Rm. 180 is access controlled. This is a good example of access control application that should be standard at all staff/faculty break rooms. Exterior windows are equipped with window treatments and obscure visibility from the exterior in.</p>	<p>General observation, this is a good example of appropriate security measures at this type of room function.</p>	0
50		<p>Classroom 171 has an exterior door that appears to have a local door alarm installed within the trim itself. Signage indicates that the alarm will sound upon exit. This door does not appear to be monitored within the access control system and if activated the alarm sounds locally only. There is no signage identifying the door number on either side of the door, the opening is egress only with no trim or key cylinder installed on the exterior.</p>	<p>Replace all battery (assumed) local alarms with hard wired, eliminate potential lack of power monitoring and battery replacement issues that standalone and wireless devices present. Apply door numbering that reflects emergency evacuation plans, use text, and finishes on signs that provide clarity and ease of reading. Remove signage that is incorrectly describing action that does not occur when the door is opened.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
51		<p>The Science building is monitored on an intrusion detection system with local video surveillance providing real time viewing capability with no storage. The cameras are not district provided. Facilities arm the intrusion system each evening at approx. 10:00 PM; there is no district exterior video surveillance monitoring of the main point of entry.</p>	<p>Recommend that all video surveillance cameras in use across campus be district provided, eliminate standalone local departmental systems that have not been approved by district for use. Potential privacy and liability issues that should be owned by the district i.e., storage parameters. Install a card reader at the arming station to provide an audit trail of who arms/disarms the system and when. Consider installation of access control at the main entry to provide remote locking/unlocking capability.</p>	3
52		<p>Level one rear access to the Science Building and the adjacent elevator landing have no video surveillance monitoring activity. The elevator remains unlocked 24/7 and is not remotely controlled by the access control system as no integration with elevator controls.</p>	<p>Install a multi-sensor camera to provide visibility of activity with a single device housing four lens. Consider interfacing the elevator controls with the access control system to allow remote locking and unlocking of elevator access on schedule. Unrestricted 24/7 access provides unmonitored areas of concealment for bad actors.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
53		<p>Science Building Rm. 202 experienced a flood causing over \$1 million worth of damage which was caused by forced entry and equipment misuse. There have been no additional security measures applied to the space post incident. Classrooms were observed with lock blocks in use during class with the doors still open. There is a lack of communication or understanding of the operational protocol regarding door position during class; they should be closed and locked when class is in session. Classroom 206 was observed with the door propped open using a trash can.</p>	<p>Apply access control measures to the building classrooms with chemical rinse showers. These classrooms should be monitored for door position based on past misuse and repair costs incurred. Install corridor monitoring video surveillance cameras. Create and distribute formalized written protocol regarding the operational expectation of doors during class. The unwritten expectation of closed and locked appears to not be followed by many.</p>	3
54		<p>Signage and lighting adjacent to the Student Services (STU) building is obscured and impeded by the tree.</p>	<p>Perform periodic maintenance of the landscaping to prevent or remove overgrown vegetation, trees, or shrubs, ensure other debris removal, maintain an unobstructed line of sight along the property paths of travel ensuring signage and lighting is not obstructed.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
55		<p>Lecture Rm. 205 is not equipped with any door position monitoring contact providing a vulnerability in the building envelopes security. The emergency exit from the library is equipped with a local door alarm. There is no door number sign present. Video surveillance is not installed at the landing, the adjacent stairwell is poorly lit.</p>	<p>Install a multi-sensor camera to provide visibility of activity with a single device housing four lens. Consider controlling the door on the access control system to allow remote lock and unlock capability, additionally terminate door position contacts on both the access control and intrusion detection systems to allow door position status monitoring. Apply door numbering that reflects emergency evacuation plans, use text, and finishes on signs that provide clarity and ease of reading.</p>	3
56		<p>Third floor exterior of the library has experienced homeless persons living on the flat roof by scaling the perimeter wall. The height of the perimeter wall is approximately 4' and there are no measures that could also potentially prevent persons within intent to cause harm to themselves from jumping. There is no video surveillance on the exterior of the building at this stairwell and landing area.</p>	<p>Install video surveillance to monitor general activity. Review options to add wall extensions (metal grilles) that would provide a barrier and deterrent for homeless persons to set-up camp on the roof. Monitor roof activity with a video surveillance camera.</p>	2
57		<p>Library third floor signage on the exit door is inaccurate as the door is locked and closed at all times from the library side. The door cannot be opened without brass key or security credential. The 2N intercom communicates directly with the library lobby (currently under renovation), providing ability for remote</p>	<p>Review the application of signage and ensure that it meets and describes the operational state. Install video surveillance to monitor elevator lobby activity.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>release of the door providing access to the elevator. There is no video surveillance monitoring activity of the intercom side or the elevator lobby.</p>		
58		<p>Signage on the door indicates that a local alarm will sound upon egress. A wall mount local alarm does go into alarm and annunciate upon exiting. The alarm can be silenced and reset by key cylinder. This alarm is extremely loud and may infringe code. At time of alarm several students occupied the library, no one paid interest to the alarm indicating a lack of direct interest or concern that security may have been breached.</p>	<p>Review the decibel output of the sounder and replace with new code compliant internal decibel annunciation unit if the existing is found to exceed indoor recommendations. Consider the interface of the local door alarm with the access control system and program the alarm to silence on closure of the door.</p>	3
59		<p>Exterior roof access stairs are accessible behind a padlocked gate leading up to the Science building rooftop. The stairwell gate can easily be scaled. The elevator remains unlocked 24/7 with locking/unlocking on schedule mechanically or remotely available. Video surveillance is lacking in this area to provide visibility and serve as a deterrent to people who may be considering bad behaviors.</p>	<p>Install a multi-sensor camera to provide visibility of activity with a single device housing four lens. Use analytics to identify activity at the stairwell providing camera call-up on motion. Consider interfacing the elevator controls with the access control system to allow remote locking and unlocking of elevator access on schedule. Unrestricted 24/7 access provides unmonitored areas of concealment for bad actors.</p>	3
60		<p>The seating area outside of the Cafeteria has two wall mount monitors that are non-operational, network and power cables are easily accessible. The seating area provides opportunity for eyes on activity and natural surveillance. The vending machines have been vandalized with no recourse as</p>	<p>Remove or reinstate the monitors to an operating state that supports Rave Alert notifications to be displayed when made. If the monitors are deemed no longer needed, remove all associated cable, and close the network data port to avoid potential cyber penetration attempts by direct</p>	4

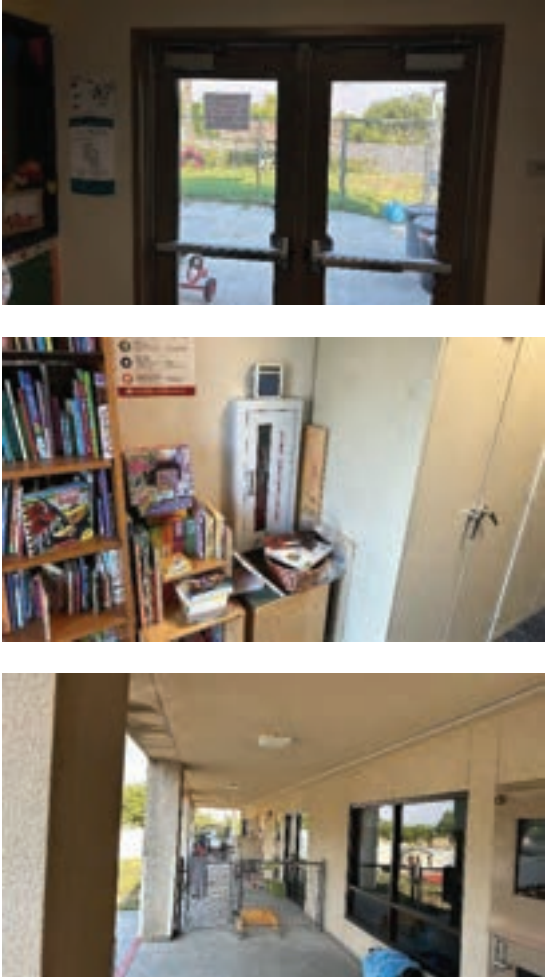
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>there is no exterior video surveillance monitoring activity that can be used forensically. Potential risk to the district network could occur as there is unsecured access to data ports available on the public side of the building, it is assumed that the data ports are not active.</p>	<p>network cable connectivity. Vending machines should be monitored by video surveillance in case of theft or vandalism forensic review needs.</p>	
61	   	<p>Exit doors at the cafeteria have signage on them indicating that these doors are to remain unlocked during business hours. Free egress is always maintained. Panasonic video surveillance cameras are installed within the cafeteria primarily observing the point-of-sale transactions. The camera system is local to the café only and video can be observed in the food services manager office. The Panasonic video system is storing approximately 10-days video.</p>	<p>Recommend that all video surveillance cameras in use across campus be district provided, eliminate standalone local departmental systems that have not been approved by district for use. Potential privacy and liability issues that should be owned by the district i.e., storage parameters. Recommend that video storage be centralized and not local.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
62		<p>Cafeteria delivery door has no ability to observe persons requesting entry from the public side. The lack of spy hole or video intercom fails to support ability for occupants to identify persons on the public side prior to opening the door. This is untypical of delivery doors at kitchens.</p>	<p>Provide ability to verify persons requesting entry both visually and audibly from the secured kitchen side. Install at minimum a spyhole, preferred option is to install a video intercom allowing verification of person(s) on the public side prior to opening the door. Exterior video surveillance camera with an internal live feed stream on a wall mount monitor would allow visibility of the wider approach and area of the opening.</p>	4
63		<p>The facilities and warehouse yard is surrounded by a perimeter 6' chain-link fencing which is easily scalable. The manual roller gate often remains open rather than being closed and secured daily. There is a standalone Panasonic video surveillance system installed at the facilities warehouse with viewing capability restricted to local staff only. Access into the facilities office is by brass key with no access control measures in place. An intrusion detection system is armed and disarmed using manual code. Parking spaces are identified for authorized use with physical signage.</p>	<p>Close and secure the gate each evening to restrict accessibility into the yard. Recommend installation of access control to reduce brass key distribution and retrieval issues and provide controlled entry on permissions basis. Add a card reader at the intrusion arming station to eliminate the need for codes that can be shared and provide an audit trail of activation etc. This should be a district and college standard approach. Recommend that all video surveillance cameras in use across campus be district provided, eliminate standalone local departmental systems that have not been approved by district for use. Potential privacy and liability issues that should be owned by the district i.e., storage parameters. Recommend that video storage be centralized and not local.</p>	2

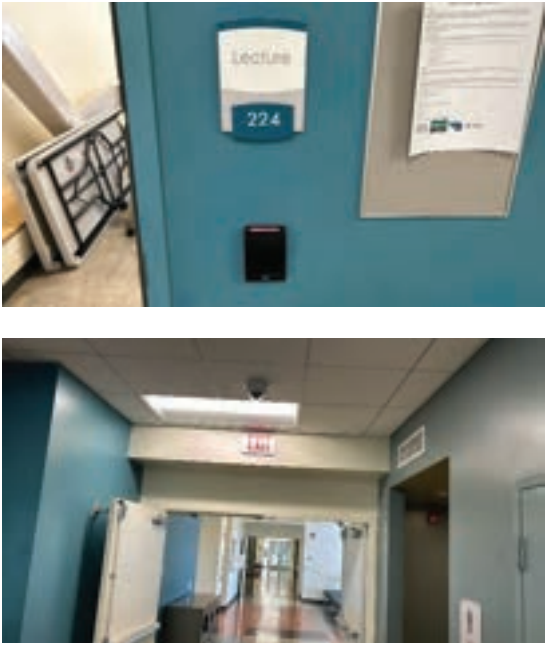


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
64		<p>Signage indicating permitted parking is positioned at the exterior of the parking lot. A-signs advising which parking bays to be used by staff, students and visitors can easily be removed, there is no fixed signage that articulates the same directions installed. Signposts appear to have had fixed signage removed, the signage should be reinstated, or the posts removed. The emergency telephone is located in the corner of the parking lot, it is easily identified during hours of darkness as the blue strobes are illuminated. Blue strobes appear not to be illuminated during the daylight hours.</p>	<p>Add additional fixed signage indicating approved parking lot usage, A-signs should be secondary means of communication. Reinstated removed signage or remove posts that present negatively on appearances as their removal if not required appears an afterthought. Strong maintenance promotes a positive image that people care about the environment, in turn this supports development of pride and a positive culture. Review programming and power at all emergency call stations with strobes, strobes should be illuminated at all times to draw attention to their location. This is a best practice approach that should be a district standard.</p>	1
65		<p>Perimeter fencing at the early childhood center is 6' in height and plastic material. Visibility into the playground area is easily achieved from points of elevation on the public side. The chain-link egress gate was found in an unlocked state providing unauthorized ingress, this is a high-risk issue that requires</p>	<p>Review the center perimeter and consider installation of an 8' chain link fence with visibility slats to restrict observation of the play area from the elevated public sidewalks. Video surveillance should be installed to provide situational awareness and forensic video review capability. The egress gate</p>	4

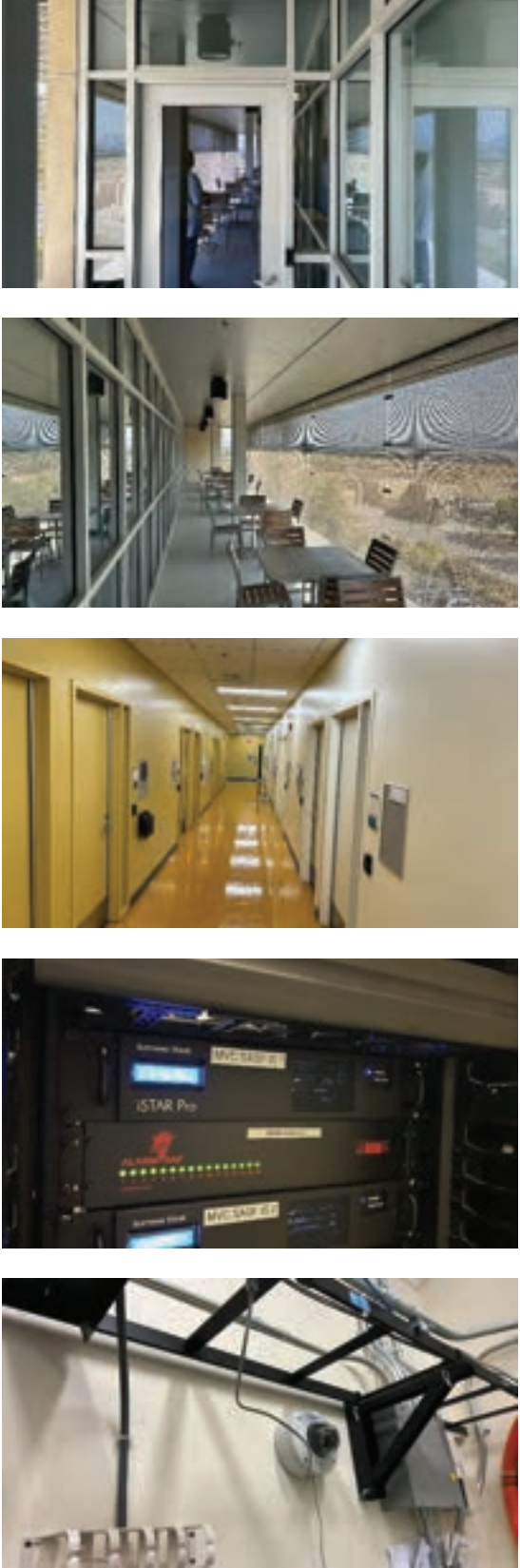
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>correcting. The center manager was notified of the gate status, the gate should remain locked from the public side. There is no monitoring of the gate position or local alarm installed that annunciates when the gate is opened. Video surveillance is not installed internally or externally. The center evacuation muster point is located adjacent to the building, and easily identifiable with signage.</p>	<p>should be closed and locked from the public side at all times. Install gate monitoring with surface mount contacts, interface with video surveillance and install a local door alarm that provides annunciation on opening.</p>	
66		<p>Lighting on the sidewalk of the early childhood center is appropriate. There are window treatments installed on the interior side of the windows restricting visibility from the public side. The gas mains are not protected with any protective caging. Visibility of the ADA drop-off area and parking lot are not supported by clear lines of site from the interior reception space or use of video surveillance.</p>	<p>Consider protection of the mains with a cage secured with a breakaway lock. Refer to local AHJ for access compliance issues. Provide visibility of parking lot activity and pedestrian approach using video surveillance and live stream video feed to a monitor in the reception area.</p>	1
67		<p>The main entrance to the early childhood facility lacks prominent and distinguishing main point of entry signage. The main entry door remains unlocked throughout normal business hours placing reception desk occupants in positions of vulnerability. The entry lobby area requires remote release of the inner access door for authorized access. There is no lockdown capability at the building as exterior doors are not electrified, panic buttons are also no present. Exterior gates on both sides of the</p>	<p>Review the lack of building identification signage, install signage that with text size, style, color, and font consistent with other buildings across campus to generate a sense of culture, belonging, and identity. The ECHC building is non-descript in appearance and should be prominently identifiable by campus users. Both exterior gates identified should be closed and locked from the public side, reference recommendation #65 for security applications. Install access control at the main entry with internal remote</p>	4




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>center were unlocked at time of observation, reference observation #65 for concerns. There are no internal telephones within classrooms and communication in a lockdown relies upon the walkie-talkies for immediate local communication. Staff shared concerns over reliability of the walkie-talkies which were a local purchase off of Amazon and not district provided.</p>	<p>release/locking of doors provided. Install a video intercom to allow reception desk staff to communicate and verify persons requesting entry prior to granting access, the main entry door should remain closed and locked at all times. Provide hardwired panic buttons at the reception and center manager office. Telephones should be provided in all classrooms and existing walkie-talkies replaced with more robust district provided units. There are potential liability issues and responsibilities by providing their own equipment that the center staff should offset onto the district.</p>	
68		<p>Internal classroom doors are stable Dutch door style and equipped with lock blocks. Internal glazing does not have window treatments applied, exterior facing windows have blinds available. Expectation is that teachers use the walkie-talkies when in the playground with children to communicate with the main reception desk if assistance is required. At the time of assessment, teachers were not using the walkie-talkies when supervising the playground activity. Procedural expectation and follow through was lacking. There is no internal or external public address system available. The main entry door is equipped with a lock blok, but the latch was retracted. This makes no operational sense as a key is needed to secure the door in a lockdown rather than immediate latching occurring upon retraction of the lock blok if the hardware remains in a locked state.</p>	<p>Review, reinforce, and provide training as necessary on basic operational expectations and use of walkie talkies and other safety and security measures. Install window treatments on the corridor facing windows. Refer to recommendation #67 reference the main entry door proposed operation, the door should be in a locked state at all times.</p>	3




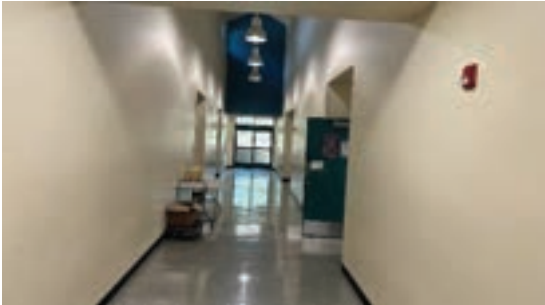
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
69		<p>Exit doors are monitored after hours when armed by the intrusion detection system. The doors can be dogged from the interior. The fire alarm extinguisher was obstructed by storage units restricting ease of access, this is not compliant with code. The playground overhang area provides cover for the homeless to occupy, staff confirmed issues with trespass and finding trash and other paraphernalia frequently. There are no trespass or regulatory signs installed. Members of the public have been observed looking into the playground from the exterior vantage points.</p>	<p>Remove the dogging feature of exterior facing doors. Remove storage items that obstruct the accessibility of the fire extinguisher. Install exterior fixed signage that clearly defines playground usage, apply regulatory bylaws and penal code that support prosecution of trespass and unlawful activity. Use text and finishes on signs that provide clarity and ease of reading.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
70		<p>SAS building administrators' office area is open access at this entry which is unlocked on schedule. All individual offices require access control credential to enter. There is no video surveillance monitoring internal activity or ability to lock the entry door via lockdown button.</p>	<p>Consider restricting public accessibility to the college executives and administrators' offices. If public or students require access to administration, appointments, or ability to communicate with person(s) prior to allowing access should occur by installation of a video intercom with call options available. Each office should be provided a video master station to support two-way audible and one-way visual verification. Video surveillance should monitor internal corridor activity.</p>	3
71		<p>Lecture room 224 at the SAS building is access controlled with a lock blok installed. At the time of assessment, the lock blok was activated and the door was not fully secured and found ajar. The room was unoccupied providing opportunity for unauthorized person(s) to gain entry and loiter detected. The lack of monitoring of the access</p>	<p>Formalize operational status of door positions and communicate and train staff to reinforce positively the intent of expectation from a safety and security perspective. Recommend that a dedicated security systems administration position be created to allow maximization of investment in existing security systems, and</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>control system provides no response to a door held open alarm event. There is inconsistency in application of door position monitoring contacts at interior access control doors. A ceiling mount video surveillance camera provides field of view of general activity within the corridor. It does not capture activity at the setback restroom openings.</p>	<p>alarm event management occur. Lock blok use at monitored doors creates system alarm events and a programming review is recommended. Replace the existing fixe field of view camera with newer technology i.e., multi-sensor enhancing visibility using existing infrastructure.</p>	
72		<p>Room 206 is equipped with access control measures; the door was held open using a lock blok band. There is no internal corridor window treatments applied to the interior side. There are window treatments on the exterior glazing.</p>	<p>Remove the lock blok band and replace with a lock blok. Bands should not be used as they require opening of the door to remove, a step that is not required when using the lock blok. Consider installation of window film on all door window vision and side panels to restrict visibility in from the public side, frosted film would minimize impact on natural light and does not require to fill glazing from bottom to top.</p>	2
73		<p>Facilities department lounge on level 3 is accessible by access control credential. There is a controlled entry providing access to the patio, free egress is maintained at all times, no video surveillance is present. Exterior card readers are redundant and should be removed. There is no exit sign above either of the patio egress doors. All office doors are access controlled with no visibility with video surveillance of corridor activity available. The IDF houses the Software House access control system server, a</p>	<p>Install video surveillance at the patio to provide situational awareness monitoring. Observation of the office corridor is also recommended. Review AHJ needs to identify egress openings and apply 'Exit' signage if required.</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>Sony camera monitors IDF activity.</p>		






ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
74		<p>Stairwell entry provides exit on the first floor only. There is no signage providing instruction to exit at the first level. Signage on the door does indicate that no reentry is possible. Access to the roof space is access controlled. There is no video surveillance monitoring activity within the stairwell.</p>	<p>Install signage reinforcing the operational intent of egress at the first floor only upon entering the stairwell. Video surveillance is recommended in all stairwells where concealment by bad actors could occur.</p>	2
75		<p>An ATM in the SAS cafeteria area is visible from the public side at night. There is no video surveillance monitoring either ATM transaction activity or general exterior activity.</p>	<p>Consider installation of window film on all door window vision and side panels to restrict visibility in from the public side, frosted film would minimize impact on natural light and does not require to fill glazing from bottom to top. Frosted film also restricts visibility at night when lights reverse the reflective capabilities of other films. A video surveillance camera should monitor ATM activity.</p>	2
76		<p>The faculty offices at the Humanities building are not controlled with access control. Brass key is required to access each individual faculty office. Window treatments are installed covering the office door window vision panels, the main entry glass has no window treatments applied. Internal video surveillance is not present.</p>	<p>Install spyholes in office doors to allow verification visually of person(s) in the office lobby area. Video surveillance camera installation would provide situational awareness and forensic review capability.</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
77		<p>Inconsistency in the application of window treatments is illustrated at classrooms 108 and 110. One room has visibility restricted and the other not (108). At the time of assessment room 108 was occupied with a class, the door was not fully closed and secured, and the door was resting on the lock blok. This is not the operational expectation of door position during class at the campus.</p>	<p>Formalize operational status of door positions and communicate and train staff to reinforce positively the intent of expectation from a safety and security perspective. Review door window vision panels and consider a standard application of district provided visibility considerations. Currently there are individual staff/faculty measures in place that do not present a controlled and consistent approach to security.</p>	4
78		<p>The egress opening at lecture room 109 is equipped with a lock blok. There is no need for a lock blok to be installed on egress only doors as they can incorrectly be propped open providing vulnerability to the space.</p>	<p>Remove the lock blok, egress only doors should not have lock blocks installed.</p>	3
79		<p>Humanities level 2 exterior entry sliding doors cannot be locked down remotely as they are not connected to the access control system. In the event of a lockdown, someone has to physically approach the doors and lock them from the interior. An example of a lock blok being installed and used incorrectly was observed at Rm. 320, as the door was propped open using door wedge. There is no video surveillance in the corridor areas. The roof hatch is not monitored for position status.</p>	<p>Consider controlling the door on the access control system to allow remote lock and unlock capability. Consider securing the roof hatch with a breakaway padlock and monitor position with a surface mount monitoring contact. Formalize operational status of door positions and communicate and train staff to reinforce positively the intent of expectation from a safety and security perspective.</p>	4


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
80		<p>Access to the faculty offices on the third floor is unrestricted as the exterior door is unlocked. Access into each individual faculty office requires a brass key. The photocopier machine was freely accessible to anyone who entered the lobby space. There is no video surveillance monitoring lobby activity. Faculty offices doors are accessible by retracting the deadbolt latch, door levers remain in a locked position. Window treatments and telephones are provided in faculty office spaces.</p>	<p>Install spyholes in office doors to allow verification visually of person(s) in the office lobby area. Video surveillance camera installation would provide situational awareness and forensic review capability. Secure the photocopier on the same keyway as the faculty office entry door restricting misuse by persons not permitted to use.</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
81		<p>The Network Operations Center (NOC) is discrete in appearance and access is controlled through restricted permissions. Access control card readers provide authorized entry at two openings, PTZ video surveillance cameras monitor general activity. There is uncertainty of who has video viewing access, and split opinion on if the cameras are operational or not. One camera is mounted adjacent to a wall mount enclosure and field of view obscured. There is no viewing monitor installed on the secured side, and no spy hole in the door to allow visibility of persons attempting/requesting entry. Windows do have window treatments applied. The building is monitored on an intrusion detection system that can be armed and disarmed at several locations within the building.</p>	<p>Review the existing video surveillance cameras and confirm if operational or not, replace if non-operational. Provide internal viewing capability. The non-discrete appearance of the building is appropriate and does not draw attention to itself.</p>	2

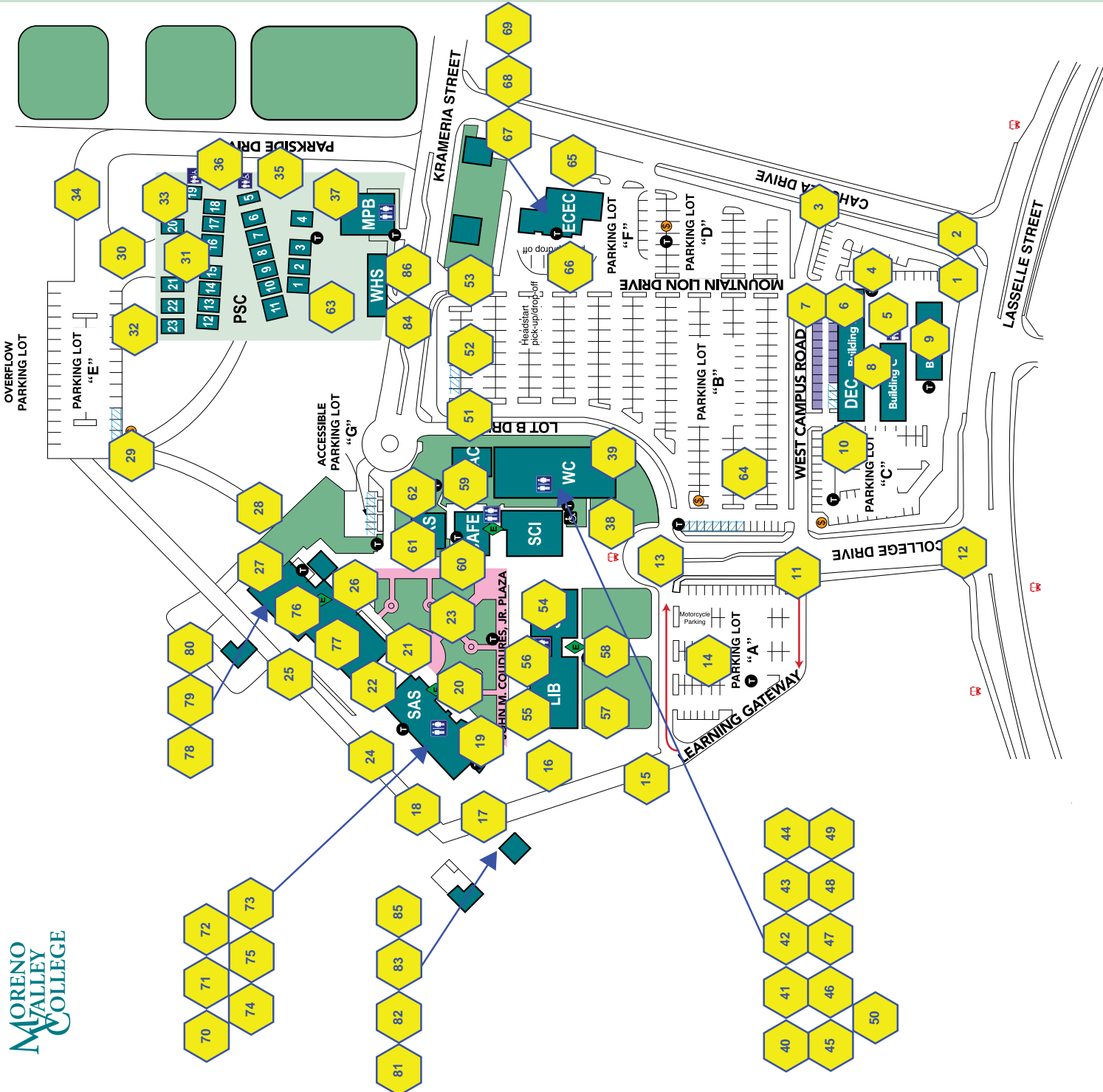
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
82		<p>Access into the network equipment control room is restricted permissions. Within the space there are several video surveillance cameras. Equipment racks were not secured and observed with keys in the cylinders and some racks unlocked and unmonitored. Security head-end servers are installed within the space.</p>	<p>Racks and enclosures should remain closed and locked, access to these should be restricted key issuance. Recommend installation of a lock box inside the secured space with code required to access keys. Keys should not be available for use by unauthorized persons if they breached the access control measures.</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
	    			

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
83		<p>The Emergency Operations Center (EOC) is in its infancy and currently equipment and space layout is under development. Laptops with role specific information are under profile creation, the space is equipped with restrooms, HVAC, generator back-up and is able to support a prolonged emergency response scenario. Television access to news channel feed and a white board for incident management are available.</p>	<p>Consider display of the proposed physical EOC layout via a wall map/sign similar to evacuation plans, supporting efficiency in setting up a physical workspace when required.</p>	2
84		<p>Identification badges are not mandated to be worn and displayed by staff and faculty. ID badges are not issued with a photograph, the example provided has been created by the provider to display his photo image.</p>	<p>Review policy and protocol regarding issuance and display of staff/faculty identification badges. Lack of identity badge policy and display makes it challenging to identify persons who belong on campus in positions of authority etc. There is no standard process in place across RCCD that provides a common expectation and ease of identification of college/district/campus staff and faculty. ID badges can create a sense of belonging, community, and encourage approach by students in need of identifying college personnel who they need to engage when</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			they have support needs or general inquiries.	
85	 <p>The first photo shows an open white storage door leading to an interior area with various equipment. The second photo shows a chain-link fence gate with a blue tarp in the foreground. The third photo shows an outdoor area with power generator units and associated piping. The fourth photo shows a fenced-in utility area with electrical equipment.</p>	<p>Access to the power generator area is easily achieved by scaling the perimeter chain link fence. Storage areas are unlocked and remain in this state 24/7. There is no video surveillance coverage of the general area which has experienced equipment theft including a golf cart.</p>	<p>Install video surveillance to provide deterrent and monitoring capability. Secure open storage areas to restrict ease of unauthorized access, consider monitoring the access gate for position with a position monitoring contact connected to the access control and intrusion detection systems.</p>	2


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
86		<p>NEC telephone handsets are available in faculty and staff offices only, they are not provided typical within classrooms. The phones do not support intercom capability and are near end-of-life. The district NEC PBX is to become unsupported by NEC at the Fall period, this may impact communication performance significantly.</p>	<p>Consider provision of VoIP telephones in all classrooms and learning areas. Reliance upon personal cell phones for communication purposes has risk if there is a cell coverage issue. Consider a Cisco or similar solution with new handsets that support wide area broadcast with intercom capability.</p>	4







- BKS BOOKSTORE**
- CAFE LIONS DEN CAFE**
- DEC DENTAL EDUCATION CENTER**
Building A - Dental Clinic
Building B - Faculty and Staff Offices
Building C - Lab, Lecture, Faculty and Staff Offices
- ECEC EARLY CHILDHOOD EDUCATION CENTER**
- HIM HUMANITIES**
Academic Success Center (ASC)
Classrooms
Faculty Offices
Workforce Prep/Ca/Works/ACES/TRIO
Vice President, Planning and Development
- LIB LIBRARY**
Dean, Student Success and Academic Support
Disability Support Services (DSS)
Library
Middle College High School Office
- MPB MULTIPURPOSE BUILDING**
Lockers and Showers
- PSC PARKSIDE COMPLEX**
1. Campus Police/Parking Services
2. Faculty Offices
3-4. Classroom
5. Restroom
6. Student Health and Psychological Services (SHPS)
7-10. Classrooms
11. Music
12. Classroom
13. Veterans Resource Center
14. E.O.P./S/CARE/NexUP
15. Dean of Instruction, Career and Technical Education (CTE)
16. Classrooms
17. Monty's Market/TRIO
18. Classroom
19. Medical Assisting Classroom/Lab
20. CTE Faculty
21. Classrooms
22-23. Classrooms
- SAC STUDENT ACTIVITIES CENTER**
ASMVC Student Government
- SAS STUDENT ACADEMIC SERVICES**
Assembly Room
Classrooms
Coffee Club
Dean, Institutional Effectiveness
Dean of Instruction, Communications and Liberal Arts
Dean of Instruction, STEM
Engagement Center
• Business, Health and Human Services (BHHS)
• Visual and Performing Arts (VPA)
Faculty Offices
Faculty Work Room
Meeting Rooms
President
Supplemental Instruction
Vice President, Academic Affairs
Vice President, Business Services
Vice President, Student Services
- SCI SCIENCE AND TECHNOLOGY**
Classrooms
STEM/IMAKE Innovation Center and MakerSpace
TRIO
- STU STUDENT SERVICES **UNDER RENOVATION****
- WC WELCOME CENTER**
Admissions and Records
Career and Transfer Center
Counseling/Financial Aid Counseling
Dean, Enrollment Services and Engagement
Dean, Student Development and Wellness
Dean, Counseling and Specially-Funded Programs
Engagement Centers
• Communication, English and World Languages (CEWL)
• Humanities, Education, Social and Behavioral Sciences (HESBS)
• Science, Technology, Engineering and Mathematics (STEM)
Evaluations
Faculty Offices
Meeting Rooms
Student Financial Services
Student Employment
Outreach/Educational Partnership
Common Ground Center/Program Offices
• Dream/LGBTQ+ Pride Center / Puente / UMOJA
- WHS PSC WAREHOUSE**
Facilities Offices and Mallroom

Norco College

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>Rodeo Road was recently resurfaced, the blue tarmac reflector indicate the location of the fire hydrant. Signage indicates that this is a fire access road and parking is not permitted, this is a single sign along the roadway.</p>	<p>Recommend that the curbstone be painted red to indicate a fire lane and no parking permitted. This may not be a requirement as the campus is private property, but consistency with other areas of campus is encouraged.</p>	1
2		<p>Removable bollards are secured with padlocks and keys to the bollards are located within the wall mount Knox box. The roller gate at F1 building is chain-link and approximately 6' in height. There is a gap underneath that provides ease of access via crawling underneath, there is no video surveillance monitoring activity that would allow for use of analytics to identify unusual activity.</p>	<p>Consider future chain-link fencing and gate heights to be a minimum 8' with ability to crawl underneath eliminated. The removable bollards and Knox box are excellent measures restricting unobstructed vehicle access around campus. Install video surveillance for situational awareness and forensic viewing capability.</p>	2
3		<p>A siren system is installed on top of the Science and Technology (ST) building. This is the predominant exterior means of communication in an emergency situation with canned messaging programmed for annunciation. There is ability to annunciate verbal communication manually from the control location in the Operations Center (OC). This system is tested quarterly.</p>	<p>The availability of mass communication is excellent, this is restricted to the exterior only. Consider use of a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. Telephones are installed internally across campus although the intercom feature is not supported by the current system set-up. Consider use of new handsets that support intercom functionality</p>	0

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			in lieu of deploying an internal public address system (PS is preferred).	
4		M1 and M2 buildings are used by facilities for storage. Access into both buildings is unrestricted during the normal hours of operation. There are no security electronics installed at either of these buildings; with no perimeter barriers or fencing restricting accessibility to both spaces.	Recommend that all facilities storage areas where financially viable be secured within an initial perimeter layer consisting of fencing and gates. At minimum buildings should be secured and access achieved either by authorized brass key issuance or alternately install access control measures i.e., card readers. Install video surveillance to monitor general activity.	2
5		The water main is protected with a metal cage. This cage is difficult to remove to perform maintenance work as the ground covering has grown through and within it making movement of the cage challenging.	Consider securing access to the mains with a breakaway lock on the protective cage cover. Refer to local AHJ for access compliance issues. Perform periodic landscaping maintenance to reduce ground covering overgrowth to below 2', perform immediate action to clear the overgrowth impacting the existing cage. Utilize CPTED best practices.	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
6		<p>General landscaping maintenance is excellent across campus, with tree canopies above 6' maintaining natural surveillance and unobstructed ability to have eyes on activity. There are some trees that do require some additional maintenance and cutting back, these are anomalies. Paint on the curbstone indicating the fire hydrant location is weathered/sun bleached and needs refresh.</p>	<p>Refresh curbstone markings with new paint. Perform periodic landscaping maintenance to maintain tree canopy heights above 6' in height.</p>	1
7		<p>There is a lack of signage on the exterior facing doors at the Applied Technology (ATEC) building that would correlate with an evacuation plan supporting first responder response. Glazing on the second level has reflective film measures applied eliminating visibility from the exterior in. There is no exterior video surveillance monitoring general activity or supporting incident response and forensic review.</p>	<p>Apply door numbering that reflects emergency evacuation plans, use text, and finishes on signs that provide clarity and ease of reading. Install video surveillance to eliminate campus visibility blind spots and support situational awareness and forensic viewing.</p>	4
8		<p>The chiller storage yard has no video surveillance monitoring activity. There have been no reported issues of vandalism or breaching the space perimeter to date. The minimal implementation of video surveillance across the entire campus, impacts monitoring of general activity or supporting</p>	<p>Install video surveillance to eliminate campus visibility blind spots and support situational awareness and forensic viewing. Installing cameras on the ATEC building would minimize footprint and maximize coverage if multi-sensor or dual-head cameras used.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		incident response and forensic review.		
9		The campus backs up to the Naval Base which is separated by perimeter fencing. There is understood to be an MOU agreement with the Navy that allows emergency access onto base in the event of an emergency. This access requires County Sheriff engagement to accompany the access onto the base if needed.	Review and ensure that an MOU is still in place. If not engage appropriate stakeholders, review, revise, and implement to ensure that the evacuation route and protocol is agreed and understood by all parties.	4
10	 	The high voltage electrical transformer is accessible as the enclosure gates are damaged and appear not to close fully and securely. As observed at the chiller there is no video surveillance.	Perform corrective action to ensure that the gates close and can be secured, eliminate the risk of danger of unauthorized entry. A single multi-head camera corner wall mounted would support visibility of several areas within and adjacent to the enclosure. Install signage on the exterior of the enclosure indicating danger.	3
11		The removable bollard is removed for ease of access around campus by the facilities and maintenance teams. The bollards serve as a secondary means of vehicle restriction as the new bollards identified in observation #2 are the primary vehicle controls.	Reinstall the bollard when facilities and maintenance access is not required. Permanent removal suggest lack of responsibility and ownership of security measures. An inadvertent presentation of security posture vulnerability may suggest there are others to potential bad actors.	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
12	 <p>The first photo shows two white electrical transformers outdoors, one of which is unlocked. The second photo shows a cluttered hazardous material storage area with various containers and equipment. The third photo is a close-up of a white door handle with a padlock.</p>	<p>High voltage electrical transformers are not protected with caging, a padlock intended to prevent misuse and tampering was found unlocked at time of assessment. General trash at the hazardous material storage area should be removed and does not provide a positive impression relating to maintenance. Location is at the Center for Applied and Competitive Technologies (CACT) building.</p>	<p>Consider securing and protecting the transformers with cages, existing padlocks should remain locked at all times, reinforce expectations to facilities and maintenance. Conduct a disposal exercise of all trash that has gathered at this area. Clean, well-maintained spaces are more appealing to campus users than areas of trash which provide a negative impression. Install video surveillance to monitor the general area.</p>	2
13	 <p>The first photo shows a red door frame with a contact magnet. The second photo shows a roller door with a lock mechanism.</p>	<p>CACT building intrusion detection system is installed and operational. There are several openings where the contact magnet has been removed and door position monitoring contacts are not installed i.e., the roller door. Arming and disarming of the system requires manual code input, there is no automated activation of the system. Access control and video surveillance are not present at this building. Operational expectation of classroom doors across campus; is locked at all times with the lock blok engaged when class in session. This is an unwritten procedure/expectation. Evacuation plans have recently</p>	<p>Review and reinstall door position monitoring contacts at all openings where they have been removed or do not currently exist. Monitor the entire building envelope without exception on the intrusion detection system. Install as a standard card readers at intrusion arming stations to provide audit trail of activation/deactivation and eliminate sharing of codes. Develop security standards and apply video surveillance as proposed standards direct. Consider standardization across the district of use of the Everlux photoluminescent evacuation maps.</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>been updated and installed across campus. These provide clear direction for evacuation and the material used retains illumination for upwards of 60 minutes in the event of power outage.</p>		
14		<p>The pedestrian walkway space is well maintained providing natural surveillance with tree canopies maintaining an above 6' height and ground covering below 2'. Physical signage is sun bleached and the information messaging displayed no longer legible.</p>	<p>Replace the sun-bleached signage. Ensure all site signage is durable against human tampering and natural weather events.</p>	3
15		<p>Kitchen delivery area opening #103 is restricted entry with access control applied. There is an exterior doorbell that provides notification to the secured side of person(s) requesting entry. The door has a spyhole providing visibility of the person(s) requesting entry if they are stood directly in front</p>	<p>The access measures in place are good, additional improvement could be achieved by considering a video intercom allowing verification of person(s) on the public side prior to opening of the door. Use the existing exterior video surveillance camera and program live feed stream to a</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>of it. A single Sony video surveillance camera monitors the general delivery area activity. There are no security gates installed at this location and an open pedestrian access point is also available.</p>	<p>wall mount monitor providing visibility of the wider approach and area of the opening.</p>	
16		<p>The corridor leading into the kitchen area from the controlled opening has an intrusion wall mount motion sensor, and a Software House arming station that is used to arm/disarm the intrusion detection system. A single ceiling mount video surveillance camera is assumed to be non-operational, and the emergency call station appears to be non-code compliant as it protrudes beyond 4" from the wall. The installation of an external call box on the interior does not make sense. A lock blok is installed for convenience purposes only when deliveries are occurring the lock blok is used to prevent the door latching. During normal operations, the door remains closed and secured. The Software House arming station can be used to place the building into a lockdown using the keypad. There is risk in this approach as these keypads are not installed at all points where there is high foot traffic. Delay in securing the building may occur</p>	<p>Review ADA protrusion limits as they apply to the built environment. Reference: Wall mount kiosk ADA 307.2 Protrusion Limits Objects with leading edges more than 27 inches (685 mm) and not more than 80 inches (2030 mm) above the finish floor or ground shall protrude 4 inches (100 mm) maximum horizontally into the circulation path. EXCEPTION: Handrails shall be permitted to protrude 4½ inches (115 mm) maximum. Review the operational status of the camera, repair or replace if necessary to provide video monitoring. The emergency phone unit would provide more value if installed on the exterior of the space. Interface with the video system for camera call-up on call activation. Review operational needs for lockdown implementation and install additional arming stations as needed.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>if arming stations are not placed in more convenient locations.</p>		
17		<p>The buildings IDF room #113 has a Sony network video recorder installed in the network equipment rack. Software House Ultra SE access control panels and power supplies are wall mounted and enclosures locked. A video surveillance camera is monitoring general activity. The space is climate controlled with a HVAC unit set at 72°. The door does not have a door closer installed to support positive latching on closure, closers should be standard components at all access-controlled doors. An emergency push button mounted on the wall does not have a cover, and there is no signage indicating what it does when pressed.</p>	<p>Install door closers on all access control openings to ensure positive latching upon closure. Develop security standards that provide consistency in security technologies used across the district. American Dynamics is the predominant video surveillance system in use, there are other standalone systems including Sony and Panasonic in operation. Recommend installation of signage and a cover at the emergency push button to inform what the button does and protect it from accidental activation.</p>	2


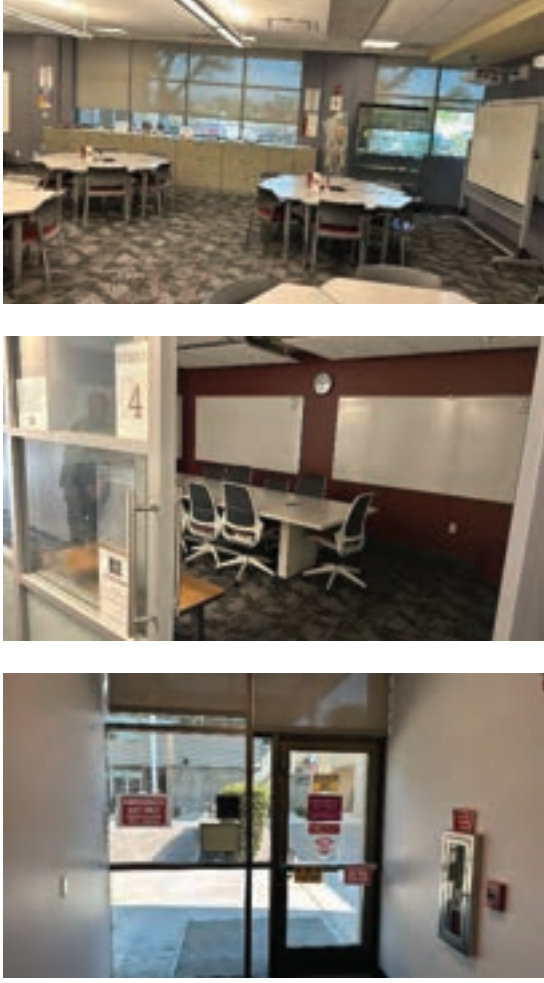

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
18		<p>The level one exterior entry into the CSS building is monitored with video surveillance and is equipped with access control measures supporting remote lockdown. An emergency phone box is wall mounted, there are different form factors of call boxes/towers in use across campus. Bollard lighting is well spaced along the sidewalk. Building identification signage is difficult to read/observe as the tree canopy obscures visibility. Reflective film applied to the glazing appears to be peeling away and requires repair to maintain its intent. The bus stop provides good natural surveillance for users as the material used as part of the structure is not solid. There are known vehicle speed issues in the parking lot which has no speed bumps or cushions in use, minimal speed limit signage is in use across campus.</p>	<p>Develop security standards that provide consistency in emergency call station type and form factors for use across the district. Perform landscaping maintenance to remove tress limbs and overgrowth that obstructs the building name from being visible. Review existing window film and mitigate visibility risks of peeling film. Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment, consider future installation of ballistic protective film. Install consistent speed limit signage throughout the campus. Consider installation of speed cushions at this location and other select locations across campus to restrict and maintain speed control.</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
19		<p>The CSS cafeteria space has a video surveillance camera monitoring the vending machines, there was an ATM installed prior to removal. There are no dedicated cameras monitoring each point-of-sale transaction counter, there are two cameras installed that provide situational awareness monitoring. Internal window treatment blinds are electronic and can be lowered as needed. These do not restrict visibility in when the lights are turned on and are primarily intended to block sunlight. Wall mounted AV monitors were observed as powered off during the assessment, these could be used to display Rave Alert notifications. Currently the Rave notifications do not appear on these monitors, there is work in progress to provide Rave notification through different visual display applications across campus.</p>	<p>Reference observation #18 regarding glazing protection. Review the AV monitors and interface the Rave Alert mass notification system to display notifications when they occur. Install as a standard approach dedicated fixed field of view video surveillance cameras above each cafeteria transaction counter.</p>	4
20		<p>Second level entry to the CSS building is controlled with access control measures for afterhours authorized access. There is a single Sony fixed field of view camera installed in the corner to the right of the entry. This camera does not provide wider visibility that a single multi-sensor camera would provide if the camera position</p>	<p>Review placement of the existing video surveillance camera. Removal of the existing camera and repurposing of infrastructure to support a multi-sensor camera would provide extensive video coverage of the entry, stairs, and general activity.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>were relocated. Newer technology using existing infrastructure would significantly improve visibility of activity.</p>		
21		<p>Student Support Services office #207 door was unlocked and can be placed into this state by presenting a security credential with permissions to unlock and lock using the two-time presentation approach. There is no internal corridor facing window treatment installed with unrestricted visibility from the corridor into the space. There is a video surveillance camera in the corridor that provides monitoring of general corridor activity, there is assumption that many of the campus cameras are non-operational.</p>	<p>Window treatments should be installed to restrict visibility from the public side, consider ballistic film. Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment.</p>	2
22		<p>An external emergency call box installed internally appears to present challenges for ADA access. The ability for a wheelchair user to access the call box without obstruction is challenging. Video surveillance cameras are installed monitoring corridor activity, see observation #21 reference operational state assumptions. Office doors are equipped with access control measures but appear to function in an</p>	<p>Reference recommendation #16 regarding mounting implications of emergency call stations on interior walls. Recommend that access-controlled offices remain closed and locked at all times, the application of access control presupposes that the intent is for the space to be secure and not accessible to the public. Create district signage standards that present a familiar feel across all RCCD campuses.</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>unlocked and propped open state during business hours. The office was empty, and computers left unlocked which presents potential vulnerability and exposure to cyber security breach. Signage on the office exterior wall clearly identifies the room number, there is inconsistency in signage style, color, and font in use across campus.</p>	<p>Design text and finishes on signs for clarity and ease of reading.</p>	<p style="background-color: yellow;"> </p>
<p>23</p>		<p>The CSS building conference room exterior facing opening #217 is identifiable with signage consistent in style, color, and font as signage in the building interior. This leads directly out to a small openly accessible courtyard area which has no video surveillance monitoring. There are ample seating areas providing natural surveillance and eyes-on-activity; however, the adjacent bamboo also provides an area of concealment and eliminates visibility of activity of wider surroundings.</p>	<p>Install an exterior video surveillance camera that monitors the seating area. Review the landscaping and consider landscaping to be a physical barrier for the building and obstruct view angles (take care not to create hiding places), but not to obstruct the lines of sight to see pedestrians or vehicles approaching the building.</p>	<p style="background-color: lightblue;">2</p>
<p>24</p>		<p>The large courtyard area provides unrestricted visibility from the elevated second level walkway leading to the Library (LIBR). There is no external video surveillance providing situational awareness or forensic viewing capability. There is no local public address system, and a damaged horn is mounted on the LIBR exterior that requires removing. The main access opening to the LIBR does not have any access control measures applied. Campus Police unlock and lock the opening daily using brass key, exterior glazing is treated with reflective film.</p>	<p>In addition to the siren system use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions both internally and externally. Exterior public address speakers at the yard area that is used for public gatherings etc., would support announcement of communications as required across a wider area. Video surveillance of this area should be installed. Consider controlling the door on the access control</p>	<p style="background-color: orange;">4</p>

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>system to allow remote lock and unlock capability. A remote lockdown button should be considered if the doors are electrified to support immediate local lockdown if needed.</p>	
25		<p>Quiet study rooms do not have the ability to be locked from the interior and windows have no treatments. The expectation in a lockdown is that all LIBR occupants on this level relocate to a safe area at the back of house area. The egress opening has a local door alarm with signage clearly indicating that the alarm will sound upon exit. The local alarm is battery operated and not monitored on any security electronics system. There appears to be no security electronics technology in use at the LIBR space.</p>	<p>Create security standards that identify the minimum baseline expectations that should be applied to district and campus buildings. Access control, intrusion detection, and video surveillance should all be in use at this location. Replace all battery local alarms with hard wired, eliminate potential lack of power monitoring and battery replacement issues that standalone and wireless devices present. Create protocol for shelter-in-place and lockdown specific to the study rooms, evacuation plans should be displayed in each room.</p>	3
26		<p>The LIBR lower-level entry doors remain in a locked state during normal hours of business and use lock blocks to allow free ingress and egress at all times. This operational state is well thought through eliminating the need for dogging of doors maintaining access with ability to swiftly close and lock doors in</p>	<p>Consider controlling the door on the access control system to allow remote lock and unlock capability. A remote lockdown button should be considered if the doors are electrified to support immediate local lockdown if needed. Install a video surveillance camera to</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>a lockdown. There are no access control measures available which would allow for remote lockdown to occur. The ATM and vending machines are not observed by video surveillance, this is inconsistent with the CSS building.</p>	<p>monitor ATM and vendor machine transactions.</p>	
27		<p>The LIBR Learning Resource Center level one access into the space is through doors that are propped open but remain in a locked state. The LIBR building has obvious high risk issues regarding lockdown as the lack of electronic hardware eliminates remote lockdown capability. There are minimal areas to shelter-in-place as many rooms are built up with storefront walls with no obscuring of visibility. The emergency exit door has several signs on it indicating that the local door alarm will sound. The alarm appears to have no power as the LED light was not flashing, as with other battery powered local door alarms on campus, non are monitored on the access control or intrusion detection systems. Window treatments are installed on the exterior facing windows restricting visibility when lowered during daylight hours from the public side.</p>	<p>Create protocol for shelter-in-place and lockdown specific to the library building. The ad hoc creation of rooms and learning spaces presents significant challenges to securing the building in a lockdown. Ability to secure the building perimeter is key maintaining, if possible, threats on the exterior of the building. Replace all battery local alarms with hard wired, eliminate potential lack of power monitoring and battery replacement issues that standalone and wireless devices present.</p>	4
28		<p>Lecture Rm. 109 door is equipped with a lock blok with door hardware that cannot be dogged from the secured side. The door window vision panel has been covered with a makeshift covering, eliminating visibility into the room from the corridor. The VoIP telephone that has recently been installed</p>	<p>Operationally review the current practice of window vision panel coverings, consider protocol that restricts coverings to 75% or AHJ recommendation that provides privacy but ability for first responders to view in. Ensure that all equipment i.e., telephones are recorded in an inventory asset management</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>into the space had been removed, this was a common issue across campus. Window treatments are installed on exterior windows and Emergency Procedures and Evacuation Plans are installed in all classrooms; this is excellent. Note: the missing VoIP telephone handset was located within a storage cabinet. There is no ability to communicate over the phone using an intercom function.</p>	<p>system, provision, and removal of communication tools such as telephones should carry consequence for removal.</p>	
29		<p>The courtyard and covered walkway areas have no video surveillance monitoring available. Internally installed emergency phone stations would provide more impact and potential benefit of installed within the exterior space, there is a lack of emergency call station installation at this area. Wayfinding and general</p>	<p>Install video surveillance to provide situational awareness and forensic viewing of the covered walkways. Install new emergency call stations strategically within the walkways providing maximum visibility to campus users for identification if needed. Install wayfinding signage that clearly identifies the direction of</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>instruction/guidance signage across campus is lacking. Direction to buildings etc. is difficult to establish due to the lack of deployment of updated campus wayfinding maps.</p>	<p>campus buildings and facilities. Use wayfinding to maintain a sense of wellbeing and security for campus users as well promoting a positive campus user experience.</p>	
30		<p>Signage to the Student Health Services Department is provided with two physical signs. These are not easily readable from a distance and are anomalies regarding wayfinding and directional signage in use on campus. There is no signage that indicates the department location from parking lots, signage is localized.</p>	<p>Reference recommendation #29 regards wayfinding, additionally consider use of digital signs and QR codes that allow campus users to use personal cell phones to self-navigate campus if digital/interactive maps are provided upon scanning of a QR code. Perform frequent landscaping maintenance to cutback growth that may obstruct signs and lights etc.</p>	3
31		<p>Accessibility into the student health services is unrestricted with no access control, intrusion detection or video surveillance installed. A door chime annunciates when the door is opened providing notification person(s) entering to staff. There is no ability for staff to observe activity on the public side approach of the space. This area often receives students with mental health issues which can easily escalate. There are no access control measures on the consultation room as observed at other locations, and no panic buttons provided. Signage on rooms does not reflect the current functionality of the</p>	<p>Discussion with staff determined that controlled entry into the space throughout the day would impede services. Visibility of the exterior approach however was a request as often agitated individuals enter the space and early awareness would be beneficial. Consider installation of exterior video surveillance with live video stream to a wall mount monitor providing the reception desk with visibility of exterior activity. Ability to automatically lockdown doors from the interior should be available along with panic buttons installed in both the main entry and the consultation room. Review and update</p>	4




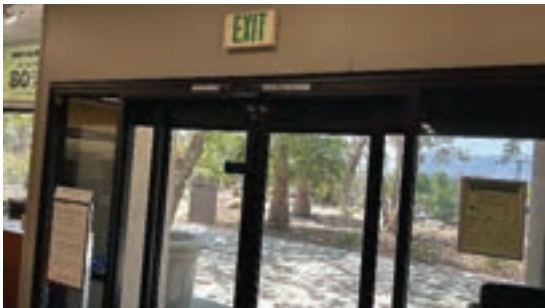
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>space. This is a high traffic area receiving between 20 and 50 patients a day. Staff in this location are vulnerable due to lack of security measures applied.</p>	<p>signage to reflect current room functionality as observed.</p>	
32		<p>The College Safety and Police Resource Center has a Software House intrusion arming station installed within it. The intrusion code for the space is unique and places this space into an armed state. A separate code can be used to implement lockdown of the building. The lockdown capability currently across campus is that input of a lockdown code will only lockdown the immediate building and not the entire campus. The same code is used for lockdown across all arming stations.</p>	<p>General observation.</p>	0
33		<p>The Police Department entrance door is on its own keyway with restricted access to Police Department Officers and staff. The Police Department has no access to the security electronics systems that are in use on campus. There is no live stream of video surveillance cameras onto monitors</p>	<p>Recommend that coordination and collaboration occur with the district police department to establish an MOU that encompasses the use of existing and future security electronics to support campus policing and incident response. The lack of visibility or use of cameras and other technologies available</p>	4


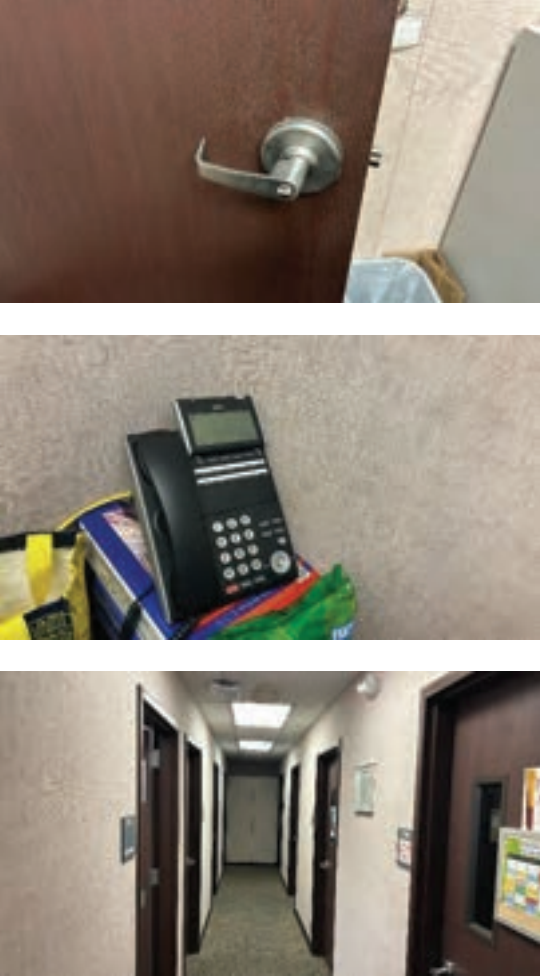
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>providing situational awareness viewing capability, and no use of remote mobile access to support incident response.</p>	<p>diminishes the investment made and ability for technology to serve as a force multiplier to existing stretched police resource levels.</p>	
34	 <p>The first photo shows a red door and a glass elevator. The second photo shows a red door with a lock block and a glass door. The third photo shows a dark doorway. The fourth photo shows a card reader and a lock on a wall.</p>	<p>The exterior elevator at the Student Services Building (SSV) cannot be locked down remotely as there is no access control system interface. This presents a significant vulnerability in a lockdown as internal access to the second level can be achieved using this elevator. The stairwell egress opening SSV 111 is equipped with a lock blok. This egress only opening should remain closed and locked at all times from the public side and used for emergency egress only. There is no video surveillance installed and the main entry doors on level one do not have access control measures applied. There is signage that indicates that no student access is allowed, this cannot be enforced as the doors remain unlocked. These doors should be controlled with access control if access is to be restricted to certain campus users. A DMP intrusion system arming station is armed by presentation of security credential at the card reader. It is understood that discussions regarding use of wireless access control measures is under consideration for the entry doors.</p>	<p>Interface the elevator with the access control system allowing for remote lock/unlock and lockdown. Accessibility from the exterior directly into the interior when all other openings are locked is a major vulnerability. A video surveillance camera should monitor activity at the elevator call buttons and the entry into SSV level one administration area. SSV 111 lock blok should be removed and the door closed and secure at all times, as an egress only door, free ingress should not be provided. The entry doors into the SSV administration space should be access controlled with hardwired options only.</p>	5

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
35		<p>The exterior facing transaction encounter is monitored with a 360-degree ceiling surface mount video surveillance camera. Interior window treatments can be lowered to reduce visibility from the public side. A mailbox installed on the concrete post is used for after-hours drop-off of payment checks etc. The built environment provides challenges to install a drop-off mailbox directly depositing checks etc. into the secure side.</p>	<p>General observation.</p>	0
36	  	<p>The President's Office is accessible from both internal and external openings, the external door is typically closed and locked at all times. Identification of the executive office is not advertised with signage which is appropriate. The office and suite have no access control measures to support immediate lockdown if required. A single panic button is installed on the conference table underside, there is no button at the reception desk (these are wireless). Access into the suite is freely available through the rear main entry reference observation #34. Door glazing has no frosting restricting visibility in. Ability to communicate with the public side if securing the suite is not possible at the suite entry as no intercom installed.</p>	<p>Entry into the executive office suite and immediate office space should be access controlled. Ability to lockdown the entry access points from within the suite should be provided. Recommend installation of a video intercom at the suite entry to support audible and visual verification of person(s) requesting entry if the suite is placed into a heightened state and operating with a secure perimeter. Hardwired panic buttons should be installed at the reception, presidents' desk, and conference table. The entry door from the administration space should remain closed and locked, frosted film applied to the door glazing to obscure visibility in. Install a video surveillance camera in the suite reception area.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
37		<p>The Financial Aid transaction counter has plexiglass that serves as a means of a barrier between public and secure side. This is clearly a remnant of the pandemic and is not intended to provide any means of security protection. There is a panic alarm installed under one of the transaction desks and another at the reception desk, these are both wireless. Video surveillance is not installed at this building supporting ability to view activity if integrated with the access control and intrusion systems for camera call-up on activation of panic button.</p>	<p>Consider deployment of hardwired panic buttons at all transaction workstations. Recommend replacement of the plastic screen with fixed glazed transaction pass through windows, the existing built environment may impede this from occurring. Video surveillance should be installed to provide situational awareness of activity.</p>	4




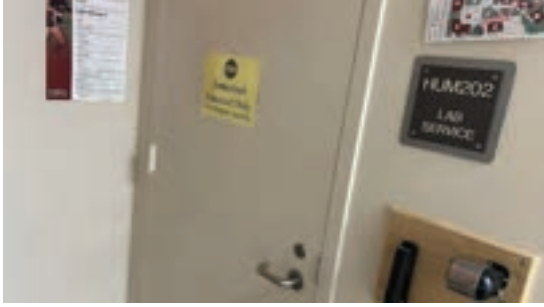
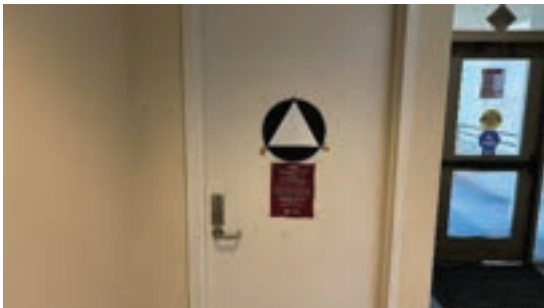
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
38		<p>SSV 222 office door hardware cannot be locked from the interior side. The exterior trim needs to remain in a locked state at all times, there is risk of doors being unlocked and not reinstated to a locked state by office users.</p>	<p>Recommend that a district standard be created that provides internal locking capability at all offices and classrooms. The need to secure a door from the exterior side in a shelter-in-place or lockdown event should be mitigated.</p>	3
39		<p>The balcony on the SSV second level presents potential security privacy issues as monitoring of activity on the level one employee/staff computers could easily occur. The second level has a DMP intrusion arming/disarming keypad with associated card reader. There is assumption that the card reader is not connected to the Software House access control system software and is programmed in the DMP system.</p>	<p>Potential observation of workspaces to extract passwords and other confidential information from the balcony may appear slim but is still an identified risk. Enclosing the balcony is not financially viable for the risk probability occurring. Application of frosted film on the balcony glazing would mitigate against potential direct observation of workers desktops from the computer work stations on level two. Communication and reinforcement of best practices regarding computer management is recommended to promote and reinforce the</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>collective responsibility, to maintain safety and security both from physical and cyber perspectives.</p>	
40		<p>The second level exterior landing provides free ingress to the counseling area via access from the exterior (see observation #34). In a lockdown the trash can is used to block the ability for the elevator to return to level one, there is no written protocol regarding elevator security in a lockdown.</p>	<p>Reference recommendation #34 regarding elevator security proposals. Install video surveillance to monitor elevator landing and stairwell activity.</p>	5
41		<p>The Trigon emergency call station located at the Bookstore is end-of-life and no longer supported by the manufacturer. The independent strobe is not illuminated providing visual identification of the call stations location. A sign indicates the emergency phone location, but text is small, and the sign is a secondary notification measure. There is inconsistency in the application across campus reference the type of devices and form factor used for emergency call stations. There is no video surveillance integrated with the call stations providing camera call up capability.</p>	<p>Consider use of a standard Code Blue all-in-one call station with blue strobe unit in the future. Use the Code Blue towers to support video surveillance cameras, solar back-up, and other devices as appropriate. Interface the Code Blue call stations with other security electronics systems providing camera call-up and notification when a call is activated. A district standard should be created, out of service stations should be covered/removed and 'Out of Order' signage installed. Non-operational units present liability risk to the college and district that should be avoided.</p>	4
42		<p>The Bookstore is a district owned building rented out to Barnes & Noble. Barnes & Noble utilize their own security system i.e., intrusion detection to monitor security status, the district have no access to this. There is an ATM machine located within the Bookstore with no video surveillance installed to monitor transaction</p>	<p>Install video surveillance externally to provide general activity monitoring.</p>	2

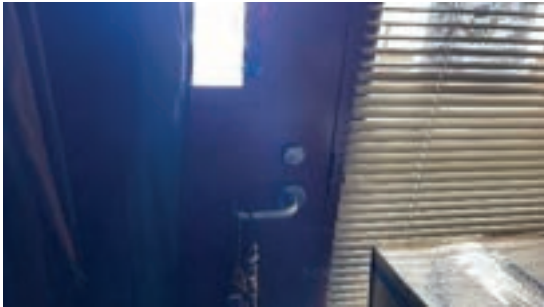
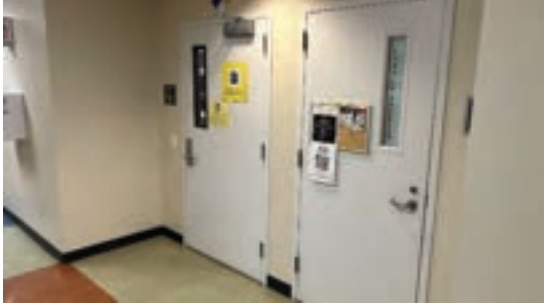

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>activity. Video surveillance is also not installed on the exterior of the building providing ability to review forensically activity if an incident were to occur. The seating area provides excellent ability to get eyes on activity and enhance natural surveillance.</p>		
43		<p>Portables A and B (Faculty Offices) are used by college faculty. Access is via brass key only with no access control measures installed. The door remains locked at all times and the space is monitored on the DMP intrusion detection system. The intrusion system is armed and disarmed by card reader suggesting that building users must have security credentials and brass keys to use access the space. Individual office doors can be secured from the inside using a push button and all have VoIP telephone phones.</p>	<p>The existing measures are adequate, recommend that future security standards determine if all faculty offices should be access controlled. Apply a standard approach to all faculty offices across campus and the district.</p>	0


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
44	 	<p>SRcomm walkie-talkie/radios are used by facilities, building and floor captains. Two different performance form factor models are used with facilities using the higher specification model on a daily basis. Written guidelines are available that provide user instruction. The campus mass notification controller is located at the Operations Center (OC). The CSC-960™ command and control system is designed for ease of use and simplicity of activation; inserting and turning the key unlocks the control panel and pushing the appropriate button activates predetermined sites with pre-programmed audible alert.</p>	<p>Radios are excellent and the consistent from factor used across campus demonstrates investment and ownership of their distribution. Recommend that the district review radios in use and select a single manufacturer to standardize on, consider roll-out of guidelines developed at Norco College as a basis for use across the district. Operational guidelines are critical to educating users and supporting confident use if called upon in an emergency.</p>	0
45	 	<p>Covered walkways at the Theater (THTR) do not have video surveillance monitoring general activity. There is a lack of video surveillance monitoring entry and exit doors at the buildings that are interconnected in this area. A Trigon emergency call station is wall mounted outside of the THTR, the blue strobe is not illuminated, and the operational state is the same as the unit observed at the Bookstore. The THTR has no security electronics applied to it. Internally the Everlux photoluminescent Evacuation Plans hold ambient energy providing visibility in the event of a power outage and</p>	<p>Reference recommendation #41 regarding emergency phone proposed considerations. Develop security standards and develop a phased upgrade and implementation program applying baseline minimum security electronics to all buildings. Consider standardization across the district of use of the Everlux photoluminescent evacuation maps.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>darkness. These are excellent and deployed consistently across campus.</p>		
46		<p>As with the THTR there is no security technology installed at the HUM. Lock bloks are installed at the main entry doors which remain in a locked state at all times, lock blok use supports positive latching upon closure. Access to classrooms uses the new Medeco key cylinders and brass keys. Each classroom has external window treatments, lock bloks and telephones provided. Note: at the time of assessment the provided telephones had been removed. The second level classroom corridor is identical to level one. Campus Police unlock and lock the building daily, there is no ability to remotely lockdown the building.</p>	<p>Develop security standards and develop a phased upgrade and implementation program applying baseline minimum security electronics to all buildings. Consider control of the entry doors by the access control system to allow remote lock/unlock and lockdown. Ensure that all equipment i.e., telephones are recorded in an inventory asset management system, provision, and removal of communication tools such as telephones should carry consequence for removal.</p>	3
47		<p>HUM01 Small Lecture room is equipped with traditional classroom hardware, lockable from the exterior only. Lock bloks are provided and the expectation is that doors shall remain in a locked states at all times. Telephone and window treatments were observed within the classroom, and an Evacuation Plan clearly posted on the interior side of the door. The door vision panel provides visibility into the space from the public side. Room signage is another example of lack of consistency in style, font size and color in use across campus.</p>	<p>Recommend that a district standard be created that provides internal locking capability at all offices and classrooms. The need to secure a door from the exterior side in a shelter-in-place or lockdown event should be mitigated. Lock Bloks and doors in a locked state is the operational expectation, internal locking removes doubt that a door may not be in a locked state if immediate locking is required. Create standards regarding signage, design text and finishes on signs for clarity and ease of reading.</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
	   			
48		<p>Gender neutral restrooms have several stalls within them, and the entry door can be locked from the interior. There is potential risk/vulnerability associated with the locking capability still present. A bad actor could lock a person(s) inside against their will. There is no video surveillance monitoring the approach to the restrooms.</p>	<p>Gender neutral restrooms with internal locking available is a high-risk situation. Recommend review of the current operation and approved use. Mixed gender restrooms with multiple stalls presents heightened risk of assaults, harassment and other nefarious activity occurring. Install video surveillance on the public side to</p>	4



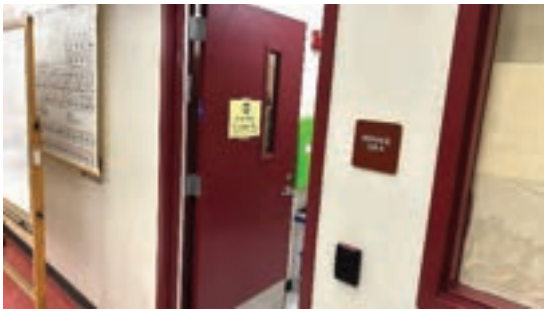
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>Evacuation Plans are removable with the frame fixed providing opportunity for refresh and replacement as needed of the map itself.</p>	<p>provide forensic viewing of person(s) ingress and egressing should an incident occur. Review alternate options for single stall all gender use.</p>	
49		<p>Faculty Office 206 accessible by brass key. Window treatments are installed and can be lowered to restrict visibility in. All office doors at this area can be locked from the interior using brass key only.</p>	<p>General observation.</p>	0





ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
50		<p>Opening ST206 at the Science and Technology Building (ST), the automatic operator push plate is not deactivated when the fire alarm system is activated providing free ingress in the event of a fire. There are challenges with exiting the opening manually due to weight and pressure implications. The door does not fit flush within the door frame upon automatic closure. A lock blok is installed that appears to impede the door closing correctly.</p>	<p>Reference recommendation #46 for connectivity to access control suggestion. Perform a maintenance review to determine if the door is within weight and pressure best practices of typical maximum opening force of 8.5 to 10 pounds on exterior openings. Verify with the fire marshal if the auto operator should be deactivated upon fire alarm, this is typically the case for fire rated doors.</p>	3
51		<p>ST second-floor observation of different examples of application of door vision panel treatments and door closers. There is inconsistency in security measures used across the building.</p>	<p>Operationally review the current practice of window vision panel coverings, consider protocol that restricts coverings to 75% or AHJ recommendation that provides privacy but ability for first responders to view in.</p>	2
52		<p>ST Faculty Offices on the second floor are accessible by brass key only with no electronic access control measures. There is no window treatment on the entry door window and side vision panel. Different faculty members have applied their own window treatments to their individual office spaces, there is no consistency in approach or mandate that window treatments be applied.</p>	<p>Review security measure expectations at faculty offices and create a single district standard. There is clear inconsistency across campus at different building faculty offices which is influenced by the time period of build. Frosted glass and internal locking hardware at these offices is proposed, installed by the college and not by individual faculty members.</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
53		<p>Engagement Center ST 107 is a converted conference room that now has been repurposed and serves student basic needs i.e., food and clothing provisions. There could potentially be issues of volatility occurring at this space, with no ability for occupants to restrict communication with the public side via video intercom etc. The entry door operates in a physically locked state with a lock blok to provide free ingress all times. Built environment conditions, restrict line of sight of activity of approach to the area, and there is no video surveillance camera installed to support real-time streaming of situational awareness into the space.</p>	<p>Install an exterior video surveillance camera with live video stream onto an internal monitor providing visibility of activity on the public side. Install access control measures to support audit check of access and apply a video intercom for audible and visual communication and verification of person(s) requesting access if the space is placed into a secure state due to heightened activity.</p>	2
54		<p>The Music Practice Rooms exterior door is unlocked and provides direct and free ingress to the three internally accessible practice rooms. Each practice room cannot be locked from the interior. There is no video surveillance on the exterior of the space or within the internal lobby area. A single VoIP telephone is available in the vestibule and tinted window film is applied to both the exterior and interior facing glazing. A drop-down blind above the exterior door is challenging to reach for anyone below 6' in height.</p>	<p>Consider controlling access with a card reader, distribute departmental credentials or issue students with credentials to restrict and control access into the practice rooms. Video surveillance should be installed on both the exterior and within the internal vestibule. Replace the blind above the door with frosted film or a blind on the entry door internal side for ease of accessibility.</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
55		<p>Natural surveillance and eyes on activity is restricted under the stairwell at the ST due to the growth of the foliage. There is no video surveillance on the building side of the stairwell monitoring activity. Restrooms are set back with no visibility of approach activity available. The women's restroom specifically is located at the end of the walkway adjacent to the stairwell overgrowth. The overgrowth presents an area of unobserved concealment that a bad actor may occupy, the lack of visibility of general activity in the area presents vulnerability.</p>	<p>Perform landscaping maintenance to mitigate bad actor concealment risk, ground covering should be no higher than 2'. Install video surveillance to monitor general activity at the stairwell and restroom areas.</p>	1
56		<p>The extensive seating area provides excellent natural surveillance and ability to get eyes on activity. Territorial reinforcement is provided by clearly defined pedestrian walkways. The lack of shade and cover potentially restricts usage of the seating areas which in turn reduces natural surveillance and</p>	<p>Consider shade structures that would encourage student use of the seating areas, engage appropriate expertise to ensure structures are not affected by winds.</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>eyes on activity. The wind is known to travel through this area at high levels and may impact any shade covering installed.</p>		
<p>57</p>		<p>Industrial Technology Building (IT) storage rooms 117A and 117B illustrate an inconsistency in the application of door closers. All access-controlled openings should be equipped with door closers as a standard feature. Door position monitoring contacts are installed at internal access-controlled openings, which is excellent. This provides ability to understand door positions and maximize security technology to support existing security staffing measures. The exit door does not have a window vision panel cover restricting visibility from the public side. The IT space has no intrusion detection system in use.</p>	<p>Install door closers on all access control openings to ensure positive latching upon closure. Develop security standards that provide consistency in security technologies used across the district. Intrusion detection at a minimum should be in use.</p>	<p>3</p>
<p>58</p>		<p>Room 117C houses the Software House iStar equipment, enclosure covers had been removed and not reinstalled. There is no video surveillance monitoring activity, again illustrating inconsistency in approach to monitoring critical infrastructure spaces. The thermostat for the HVAC system appears to have no power to it, the HVAC system is non-operational. Entry requires presentation of a security</p>	<p>Security headend equipment should be secured with enclosure doors reinstated and the enclosure status monitored by a tamper switch. Video surveillance should monitor activity within the space at minimum with exterior video surveillance interfaced with access control providing camera call-up on alarm event trigger. Engage facilities and maintenance to review the HVAC system and restore to operating state.</p>	<p>2</p>




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>credential with permissions to access the room.</p>		
59		<p>Several Sony video surveillance cameras provide general situational awareness viewing capability and approach and activity at the vending machines. A single multisensor camera would provide significantly enhanced viewing capability using existing cable if installed. The external elevators remain unlocked at all times with no interface with the access control system to support scheduled lock and unlock. Restrooms are locked and unlocked on schedule via the access control system. There is no signage indicating the hours of availability.</p>	<p>Recommend that elevators be controlled by the access control system with ability to remotely lock and unlock on schedule. Card reader at the first-floor hall call buttons would provide authorized use when in a locked state. Display signage that clearly displays the hours of operation at the restrooms. Consider an internal public address system that provides notification to restroom occupants in the event of a restroom so that they can shelter-in-place when doors are remotely locked. Video surveillance should monitor all elevator landing and restroom entrances.</p>	2
60		<p>Access control measures are applied to the Service Rm. 128–A. the door was found in a door held, propped open state with the LED on the HID card reader flashing. There is no monitoring of the access control alarm events or follow through with training to help correct poor behaviors. When the door was closed the alarm event was removed as the door contact monitoring reset the door position status.</p>	<p>Reinforce operational expectations of access control openings. Current alarm events are not observed or managed, create a systems administration role that oversees campus security electronics. Existing systems are underutilized to maximize their potential benefit to maintaining safety and security on campus.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
61		<p>Expensive 3-D printers at the IT are stored within an access-controlled storage room, which is excellent. However, there is no video surveillance installed that monitors the space contents or supports ability to interface with access control and /or video surveillance to provide camera call-up on alarm event.</p>	<p>Develop security standards and develop a phased upgrade and implementation program applying baseline minimum security electronics to all buildings. Propose that video surveillance be installed in high value equipment storage rooms.</p>	3
62		<p>A single video surveillance camera monitors activity at the seating area. A multi-sensor camera would provide enhanced visibility using existing infrastructure.</p>	<p>Consider swap out of the existing fixed field of view camera for a multi-sensor, repurpose existing cable if CAT 6, if required pull new cable.</p>	1
63		<p>The roller door in the IT building is not monitored with a door position monitoring contact. This presents a vulnerability in the building envelope security posture, and a place for potential undetected unauthorized entry. The roller door appears not to be used frequently.</p>	<p>Install surface mount door position monitoring contacts and terminate on the intrusion detection system.</p>	3
64		<p>Access control measures at the Q (IT) building appear excellent with all exterior envelope doors monitored on the intrusion detection system. There is no video surveillance within the corridor providing visibility of general activity.</p>	<p>Install video surveillance to provide situational awareness viewing capability.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
65		<p>Suite 200 at building Q (IT) is faculty offices with access control on each and every door within the space. The main entry door into the suite is unlocked on schedule and a lock blok applied with the door in a locked state all times to provide immediate latching on closure. The exit door remains locked and closed at all times, the lock blok should not be engaged. A door wedge in use at Storage Room 200–T with a lock blok strap retracting the latch indicates that the door is never fully closed and secured. The Software House keypad arms and disarms the entire buildings intrusion detection system. Lockdown can be activated by input of a code that will lock down the building only, a separate code is available that will lockdown the entire campus.</p>	<p>Remove the exterior door lock blok, the egress only door should not be propped at any time. Remove the lock blok strap and door wedge at Rm. 200-T and close and lock the door, if free ingress is required at all times remove the access measures.</p>	4
66		<p>The setback seating areas on the second floor provide potential area for homeless to sleep undetected for a sustained period. The bench provided does not include CPTED recommended seating that restricts ability for persons to lay down and sleep on furniture, deterring social nuisance.</p>	<p>Review CPTED best practices regarding external furniture an consider for future installations, limit opportunity for sleeping on benches. Install video surveillance to monitor exterior walkways.</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
67		<p>Natural surveillance and territorial reinforcement is supported by excellent maintenance and landscaping at the ATEC building. The emergency phone unit is manufactured by Trigon and no longer available. The call station instructional signage is damaged and no longer legible. The blue strobe is not illuminated, and the base is not complying with ADA requirements allowing for unobstructed or impeded wheelchair access. There is no video surveillance installed at the exterior for the ATEC building.</p>	<p>Blue strobes should be illuminated at all times for ease of identification of call stations. Future installation consider use of Code Blue towers to support video surveillance cameras, solar back-up, and other devices as appropriate. Interface the Code Blue call stations with other security electronics systems providing camera call-up and notification when a call is activated. A district standard should be created, out of service stations should be covered/removed and 'Out of Order' signage installed. Non-operational units present liability risk to the college and district that should be avoided. Review ADA accessibility needs and perform corrective actions, as necessary.</p>	4
68		<p>ATEC Classroom 119 door latch can be retracted using the key cylinder on the interior panic bar, dogging of doors should not occur. A lock blok on the interior supports a locked door at all times. Window treatments (blinds) restrict visibility from the public side when lowered.</p>	<p>Review hardware with internal dogging capability and remove key cylinders and dogging access, replace with blank plates.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
69	   	<p>Lecture Rm. 114 is monitored on the intrusion system and has a Bosch arming station, this is a separate system to the typical DMP intrusion detection system found across campus and at other locations. There is no access control measures applied to the sliding entry doors and video surveillance is not installed. The desk mount AV monitors display Rave Alert notifications when made. The egress door when opened was infested with earwigs.</p>	<p>Consider controlling the door on the access control system to allow remote lock and unlock capability. A remote lockdown button should be considered if the doors are electrified to support immediate local lockdown if needed. Install exterior video surveillance camera interfaced with the access control system providing alarm event trigger camera call-up.</p>	4
70		<p>A TEC first floor laboratory exit door was found not positively latched providing free ingress. The door mount local alarm has no power rendering the intent to announce upon door opening redundant. The batteries require replacing to reinstate the sounding capability, the alarm is not</p>	<p>Replace all battery local alarms with hard wired, eliminate potential lack of power monitoring and battery replacement issues that standalone and wireless devices present.</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		monitored on the access control or intrusion detection systems.		
71		ATEC second floor women's restroom is setback without video surveillance of activity. The restroom is unlocked and locked physically by Campus Police. The fire alarm pull station is accessible for misuse and tampering with and the stairwell is a blind spot for persons entering and exiting the restroom.	Install a multi-sensor video surveillance camera to monitor restroom entrance, stairwell and second floor walkway activity. Develop security standards that provide a consistent level of security measures at restrooms, current conditions lack any standardized approach.	2
72		Rm. 209 is an Art Lab; reflective window film is applied to the exterior glazing eliminating visibility during hours of daylight from the public side in. The intent of the film at install was simply to serve as a means to reduce sunlight into the Lab, it now serves a positive impact on building security. Additional window blinds can be lowered to restrict visibility further in the evening when lights are turned on, thus eliminating the film reflective capability.	General observation, develop security standards that provide consideration of use of ballistic film on future building refresh or new construction projects.	0
73		The ATEC second floor seating area outside of the Art Lab. provides an area for eyes on activity as well as an area for unobserved loitering. There is no video surveillance providing situational awareness of any activity at the exterior of the ATEC building.	Install video surveillance to monitor activity in this area which is currently an unmonitored blind spot.	2

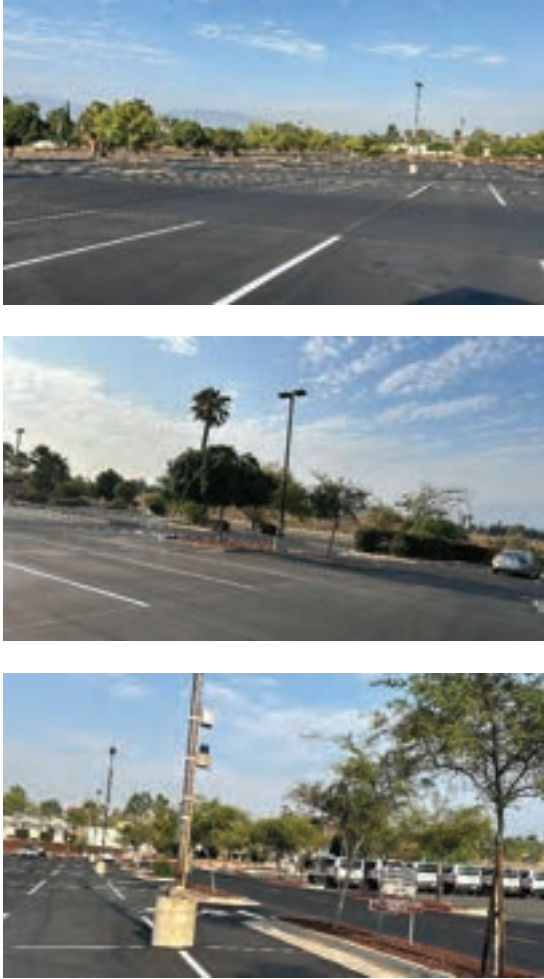

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
74		<p>Signage on the Third Street approach road indicates that parking permits are required on campus and that no parking is permitted along the roadside. Some of the signage is sun-bleached and in need of replacement. There is a lack of speed restriction signage implemented along the roadway with no speed cushions, bumps, or other measures in place to reduce vehicle speeds. Access to both the Norco College and JFK Middle College High School (JFK) can be blocked at this one way-in, one way-out road. The quantity of signage present is overwhelming, causes sensory overload, and is impossible for vehicle drivers and passengers to observe and understand on approach. The overload of information does not achieve the intent of its placement.</p>	<p>Consider a review of the signage placement and quantity. Review information displayed and determine if specific information can be relocated to other areas i.e., parking permit information relocated to parking lot points of entry. The current overload of information encourages vehicles to stop and review which is contradictory to signage displaying no parking. Sun bleached signs should be replaced with new. Consider using tarmac signage and new fixed signage that directs vehicles to select lanes for JFK school access only and other lanes that serve Norco College. Strategic placement of speed cushions is recommended to reduce vehicle speeds without impacting bus and first responder access.</p>	3
75		<p>JFK Parking Lot, signage indicating dedicated areas for students and staff within their designated parking areas is minimally displayed. The signage is mounted high up on the lampposts rather than at a height that is clearly visible and more noticeable. There are separate entrances for staff and students however this is not easily noticed until directly at the point of entry into JFK Drive. There is no tarmac or physical signage indicating the appropriate path to take for parking on Windy Way. There are speed bumps in the student vehicle entry lane but none in the staff lane. A single 15 MPH speed sign was observed in the</p>	<p>Add additional space use signage and mount at heights that are easily observable. Signage identifying separate entry lanes should be displayed on Windy Way providing early notification of the separated access roads. Reinforce the entry points with tarmac signage. Speed bumps should be installed within the staff entry lane similar to the student lane. Provide additional speed limit signage and pole mount for ease of observability. Define the student drop-off area with curbstone paint i.e., green paint, and consider installation of roll-over bollards similar to those on Third Street to separate the drop-off area and bypass lanes.</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>student entry lane at the base of a ground sign, it appeared to have been misplaced. The student drop-off area is not identified or distinguished with any paint on the curbstone.</p>		
76		<p>Signage is not consistent in its deployment, for example 'Do not enter' signage is installed on the staff parking lot entry, but not on the student and visitor parking entry. There is no signage indicating that a one-way system is in use, and some signage indicating not to turn left is sun bleached and in need of replacement. There is no video surveillance in the parking lot area and no emergency call stations installed within Parking Lot K.</p>	<p>Review the existing signage deployment and provide additional signage or remove as appropriate ensuring that a consistent message is communicate to all. Access points into both students and staff parking areas should be treated equally. Recommend deployment of 'One-way' signage to clearly communicate eh expected vehicle path of travel. Sun bleached signage should be removed or replaced with new. Recommend that both video surveillance and emergency call stations be installed; coordination between school and college should occur as the crossover of campus usage requires coordination of continual visibility from one parking lot to another. Standardization of emergency phone application is recommended.</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
77		<p>ADA parking spaces are identifiable with physical signage and tarmac signage. Some of the physical signage is weathered and in need of a refresh. The one-way traffic system and point of exit is not clearly communicated using painted tarmac signage or reinforce by physical signage.</p> <p>The bus lane is identifiable with bright yellow physical signs, however, there is no paint that indicates the separation of the bus lane from the adjacent roadway. There is a lack of signage indicating that vehicles must exit campus in a specific direction. Access to the Norco College Parking Lot B and service road is freely accessible.</p> <p>During the evening lighting assessment, it was observed that some of the post mount double luminaires only had one luminaire distributing light. This 50% use of lighting impacts the lighting levels experienced considerably.</p>	<p>Reference recommendation #76 regarding application of 'One-way' signage. Replace sun bleached signage with new. Consider reapplying yellow paint to define the bus drop off lane and distinguish this with tarmac paint. Install signage at the College Way 4-way junction that clearly indicates the exit path for vehicles to leave the school campus lot. Review the parking lot lighting and perform as needed maintenance to reinstate luminaires that were observed as without power. The reduction in lighting that is fully operational impacts the visibility across the parking lot at night significantly.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
78		<p>Parking Lot B has two pole mount emergency telephones installed. These are old GAI Electronics units no longer available. During the evening lighting assessment, it was observed that the strobes are not illuminated and there is no physical signage providing identification of their location to campus users. Signage providing instruction that white parking spaces are for students only is poorly distributed, as is wayfinding signage providing direction to campus buildings. There is no wayfinding signage in Parking Lot B. There are no vehicle barriers or other speed control measures within the parking lot that would support reduction of vehicle speed and support compartmentalization of access to campus grounds.</p>	<p>The visibility and ease of identification of the emergency phone locations is challenging. Consider use of a standard Code Blue all-in-one call station with blue strobe unit in the future. Use the Code Blue towers to support video surveillance cameras, solar back-up, and other devices as appropriate. Interface the Code Blue call stations with other security electronics systems providing camera call-up and notification when a call is activated. A district standard should be created, out of service stations should be covered/removed and 'Out of Order' signage installed. Non-operational units present liability risk to the college and district that should be avoided. Strengthen parking instruction with additional signage and provide wayfinding maps at the corners of all parking lots closest to the college buildings. Speed limit signage should be displayed consistently within parking lots and consider strategic positioning of speed bumps and cushions to support speed restrictions. Parking lots could be compartmentalized from an access perspective with installation of swing-arm barriers.</p>	4
79		<p>A single sign indicating that yellow parking bays are for staff parking only needs repair, as it is leaning over; the sign is difficult to read from a distance. The yellow markings on the tarmac require a refresh of new paint to clearly define parking bays. The parking permit dispenser is located at the furthest point away from the college with no video surveillance monitoring activity. ADA parking spaces are identified with signage on the tarmac and physical signage at</p>	<p>Perform maintenance repair and refresh of signs as identified. Install video surveillance across all parking lots providing visibility of activity and to serve as a potential deterrent to bad actors. Strategic placement of multi-sensor cameras would provide significant coverage. Use of wireless point-to-point data transmission would reduce data and power needs as potential battery; solar and step-down transformers could</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>each bay. The physical signage needs a refresh as it is weathered/sun bleached and no longer clearly displaying the message intent.</p>	<p>utilize power available at lamp posts to support the cameras.</p>	
80		<p>Parking Lot A, parking spaces and general signage within this lot are significantly stronger than those observed in Parking Lot B. There appears to have been a recent refresh of the asphalt and parking bay markings. This is excellent and presents a welcoming environment to students, visitors, and faculty etc. There are emergency call stations installed in the lot, the call stations appear to have been overlooked in the parking lot refresh. The blue strobes were illuminated during the hours of darkness for ease of identification, they do not appear illuminated in the daylight. There is no video surveillance installed in the parking lot.</p>	<p>Reference recommendations #78 and #79 for emergency call station and video surveillance considerations. The presentation of the parking lot should be rolled out across campus as it represents pride and care of the facility, which is welcoming. Wayfinding should be provided to support ease of building identification to parking lot users.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
81		<p>Parking Lot C is dedicated for student parking only. There is a single emergency telephone installed in the parking lot, which is insufficient for the size of the area. There is no consistency in the type of emergency call stations used across campus. The unit in use in this parking lot is a Trigon call station. The parking bay markings and tarmac are exceptionally well maintained. There are no speed control measures in place, including a lack of speed bumps, vehicle barriers and speed control signage. There have been instances of vehicle vandalism occurring within the parking lot areas, but no video surveillance installed to support forensic review.</p>	<p>Reference recommendations #78 and #79 for emergency call station and video surveillance considerations. Speed limit signage should be displayed consistently within parking lots and consider strategic positioning of speed bumps and cushions to support speed restrictions. Parking lots could be compartmentalized from an access perspective with installation of swing-arm barriers. Enforce use of official parking permits on vehicles using segregated parking areas (e.g., student, employee lots). Remove non-registered or illegally parked vehicles.</p>	4
82		<p>Parking Lot D has poorly defined parking bays and needs a maintenance refresh. Dedicated motorcycle parking is not clearly identifiable from a distance, and there is no wayfinding signage providing any direction to this location from the Third Street point of entry to campus. Student parking is permitted with use of a permit only. College vehicles are parked and stored within this parking lot, there is no restriction to exit campus with a vehicle if unauthorized access to one occurs. As with all other parking lots there is no video surveillance. All parking lots have a lack of speed restriction measures in place, all parking</p>	<p>Reference recommendations #78 and #79 for emergency call station and video surveillance considerations. Speed limit signage should be displayed consistently within parking lots and consider strategic positioning of speed bumps and cushions to support speed restrictions. Parking lots could be compartmentalized from an access perspective with installation of swing-arm barriers. Enforce use of official parking permits on vehicles using segregated parking areas (e.g., student, employee lots). Remove non-registered or illegally parked vehicles. Provide signage that indicates the</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>lots could be compartmentalized with use of vehicle barriers to restrict vehicle access into parking lots outside of authorized usage times. A single sign at Parking Lot D does provide some direction to campus buildings.</p>	<p>location of motorcycle parking bays from Third Street.</p>	
83		<p>The West End Drive tarmac has recently been resurfaced and paint markings are clearly defined. There are speed bumps present however, there is no vehicle speed restriction signage installed. The emergency phone is another example of inconsistency in standardization of type, the red tower is easier to identify than post mounted units. There is no video surveillance.</p>	<p>Reinforce speed limit control with physical signage.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
84		<p>WEQ Rm. W8 portable is a fitness room with entry by brass key only. There were no security electronic access control measures deployed across the portables. Room usage signage is small with minimal text not easily identifiable from a distance. Window treatments are installed and can be lowered when needed. Lock Bloks, Emergency Evacuation Plans and Procedures were installed and displayed as typical.</p>	<p>Recommend that all buildings at a minimum be monitored with an intrusion detection system. Review signage across campus and consider implementation of consistent signage style, fonts, text size that provides a standardized approach. Ensure all site signage is durable against human tampering and natural weather events. Signage can support the culture, sense of community, and be welcoming when deployed correctly. Consider signage that is consistent in appearance across the district rather than just this campus.</p>	4
85		<p>Classroom W7 is accessible by brass key, typical measures were observed including a wall mounted VoIP telephone. There are challenges across campus due to network port locations which restrict placement of telephones on the wall, which is the preferred mounting location. The Medeco brass keys</p>	<p>Consider installation of data network ports at consistent locations within new build and existing building upgrade projects. Consider a consistent location to support preferred wall mounted VoIP telephone placement. The use of the Medeco restricted keyway is excellent and should be rolled out to all openings on campus, a</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>and key cylinders are in use at these portables.</p>	<p>district standardization on keyway should be considered for ease of management, distribution, and retrieval supported by an electronic key management system.</p>	
86		<p>Gates between portables intended to restrict access to the utilities were unlocked. Even when locked the heights of the gates does not function as sufficient deterrent to scaling.</p>	<p>Gates should be secured with padlocks and video surveillance installed to provide situational awareness and forensic viewing capability. Replacing the gates with new taller gates is not recommended due to cost consideration and minimal additional deterrent provided.</p>	1
87		<p>The Activity Center is easily identifiable with its building signage. The space provides public services and there are men's and women's locker rooms. There are no access control measures or video surveillance in use. An emergency call box is mounted on the wall with signage. This is an old Trigon unit no longer supported by the manufacturer, the blue strobe was illuminated at night. The W-2 classroom is used for martial arts and dance classes, there have been instances of vandalism occurring within this room.</p>	<p>Consider installation of security electronics including both video surveillance and access control. Ability to secure this facility remotely is encouraged as it is a known area of vulnerability and concern. Internal communication capability within the restrooms visually and audibly should be considered if the rest and locker rooms are able to be remotely locked down.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
88		<p>Rm. W-2 is monitored with a local DMP intrusion detection system, the intrusion system does not appear to roll out to other portables. Door position monitoring contacts are used to monitor door forced alarms. A VoIP telephone, Emergency Evacuation Plans and Procedures, and lock blok were observed as typical.</p>	<p>Roll out the intrusion system across the entire W complex of buildings.</p>	3
89		<p>The men's locker rooms signage is weather damaged and in need of replacement. The location of the locker room on the rear of the building is adjacent to areas of concealment. There is no video surveillance providing potential deterrent to a bad actor, or ability to monitor general activity in real-time or forensically.</p>	<p>Consider installation of security electronics including both video surveillance and access control. Ability to secure this facility remotely is encouraged as it is a known area of vulnerability and concern. Internal communication capability within the restrooms visually and audibly should be considered if the rest and locker rooms are able to be remotely locked down. Replace damaged signage with new.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
90	  	<p>The water mains chain link is broken, and there is no protection provided from potential vehicle damage directly from Third Street. A sign on third Street indicates that there is a speed limit of 35 MPH. Access to the sporting area parking lot cannot be closed off as no barrier available. The light luminaire needs replacement/installation as missing.</p>	<p>Secure the mains from tampering by reapplying the padlock to the chain with the chain fully secured. Install speed limit signs along Third Street in a consistently spaced approach. Installation of speed cushions would provide speed control measures with dimensions on width that do not impede the buses and first responder access. Consider installation of a swing-arm barrier at the entrance to the sports complex parking lot entrance to support compartmentalization of space and restrict unauthorized vehicle access when campus is closed. Reinstall the missing luminaire.</p>	3
91	 	<p>The Sports Complex is open access during normal college hours, this presents potential conflict with members of the public who wish to use the facilities. There are no access control measures that maintain safety and security of students and staff by restricting public access. There is a lack of signage indicating permitted use of the complex. The parking lot facing gate is decorative fencing and approx. 9' in height. An emergency call station tower is present with no illuminated strobe during daylight hours, video surveillance coverage is not available.</p>	<p>Review with legal counsel language that can be applied to physical signage that supports enforcement of unapproved access and use. The open nature of the complex presents challenges to maintaining safety and security of authorized users. The emergency call station should be upgraded as part of a refresh of all emergency call stations across campus and the district. Review the accessibility to all approach with consideration of closing and securing public entry during college hours of use. Reconfiguration of the point of entry may be required. Public use of the facility has potential liability impact on the college if</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>an injury or other incident occurs.</p>	
92		<p>The locker and changing rooms remain open and unlocked when in use by students. The complete open unrestricted shared use of facilities is unusual and presents risk and vulnerability of misuse of facilities and opportunity for bad actors to loiter. During sporting events there is no separation of team participants, fans, and the public. There are several access points into the complex that could be used to support separation of user groups during sporting events.</p>	<p>Unlocked and shared college and public use of the facilities should be reviewed. The initial built layout of the locker and changing rooms is not suffice for current operational use. Mixed use access including children using the same unsecured spaces as adults has potential liability impact that should be reviewed. Separating access into the complex for opposing team fans, general public and others, is not viable at this time as all points of entry lead to congregation at the same area.</p>	4


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
93		<p>Access onto the field is through double chain-link gates. There are several points of egress from the field area but no signage indicating exit points. Two emergency phone towers are installed within the field area, they are not easily identifiable as the housing paint is faded so much that they blend into the background. There is one set of bleacher seating which is used by all fans (home and visiting). The perimeter chain-link fence is approximately 10' in height, neighboring homes visibility is obscured with a block wall. There is conflict between neighbors and the college regarding use of the facility. Floodlights are not installed restricting use of the complex after daylight hours, this reduces natural surveillance and ability to have eyes on activity longer.</p>	<p>Install signage that clearly identifies the exit points from the field area, where signs are to be installed ensure that free egress is always maintained, and that chains and padlocks do not impede ability to exit. The emergency call stations should be upgraded as part of a refresh of all emergency call stations across campus and the district. Recommend that additional spectator seating be provided that supports separation of "Home" and "Away" supporters. Use of multiple exit points would allow separate exit points for the fans mitigating potential conflict that may occur at sporting events. Lighting would support extended use of the facilities by the college and enhance security of the area which is unlit at night.</p>	4
94		<p>Tree landscaping adjacent to the field area is overgrown and provides several areas for bad actor concealment. A neighboring property has an access gate that provides direct access onto campus property. There are liability implications of neighboring properties having direct access into college grounds.</p>	<p>Perform periodic maintenance of the campus perimeter setbacks to prevent or remove overgrown vegetation, trees, or shrubs, maintain an unobstructed line of sight along the property boundary. Engage the neighboring property regarding the unauthorized access point onto campus directly from the property. Seek legal counsel advice, as necessary.</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
95		<p>The fence line is excellent however, there are some trees that are starting to encroach into the chain-link which will cause damage. The trees restrict visibility out but do provide a screen. There is no video surveillance or lighting that supports the college or district's ability to monitor activity within the area. Access gates are unlocked during college hours to provide additional egress for students. There are no exit signs installed on any of the points of egress. The athletic trainer works out of the trailer at this facility when on site. The trailer also houses first aid equipment, and other sporting equipment, again there is no ability to review video if attempts to steal or other incidents occur.</p>	<p>Perform maintenance of the landscaping to cutback the trees that are impeding the chain-link fencing. Install new protective covers at receptacles where currently missing or damaged. Reference recommendation #93 regarding exit signage. Install video surveillance that provides situational awareness and forensic viewing capability. Video surveillance should be installed to support potential review of sports events crowd disturbances and support monitoring of events such as graduation that takes place on the sports field. Conduct a review of operational needs of the complex, separate team locker and restrooms are recommended separating the current situation of shared use with the public.</p>	3






ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
96		<p>The emergency vehicle access gate at the Sports Complex parking lot is secured, first responders can access the Knox box for keys to unlock the gate. Neighboring properties have chain-link and block walls as means of delineating their property from campus. Painted curbstones clearly define areas of no parking which is excellent, physical signage reinforces parking restrictions.</p>	<p>General observation, provision of video surveillance would support situational awareness and forensic viewing capability, as well as serving as a potential deterrent to bad actors.</p>	0
97		<p>A horse trail runs the entire length of Third Street with open public access. A chain-link fence runs along the shared responsibility space between neighbors and the college grounds. The fence line is broken with areas of openings for public access onto the trail and subsequently the campus from adjacent neighborhoods.</p>	<p>The horse trail management is shared responsibility with city and neighbors. Consider installation of video surveillance along Third Street that provides visibility of activity both on the roadway and the horse trail area. The current lack of visibility eliminates any ability to have eyes-on persons entering or exiting campus through the</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>public openings leading into adjacent neighborhoods. Signage should be installed at the entry points onto campus that communicates unpermitted activities.</p>	
98		<p>A GAI Electronics emergency call station is located on Third Street. The wooden fencing adjacent to it is starting to rot away and in need of removal or replacement. There is no video surveillance along Third Street. There are two emergency call stations along this long stretch of road. Speed limit signage is offset to the street and the no parking signage is sun bleached, best intentions of signage placement fails to deliver the desired intent.</p>	<p>The emergency call station towers would provide increased value if relocated to the parking lots opposite. The current placement does not best serve an area of significant use such as the parking lots. Emergency call stations should be upgraded as part of a refresh of all emergency call stations across campus and the district. Install speed limit signs along Third Street in a consistently spaced approach. Adjust the existing signage so that vehicles can clearly observe on approach. Provide dog waste garbage cans and signage indicating expectations on dog walkers to not leave dog waste behind. Review the fencing and replace</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>as needed, the rotting wood leaves the fence vulnerable to failure.</p>	
99		<p>The Veterans Resource Center (VRC) is a new building accessible by access control. The main entry is unlocked when the building is occupied. Axis video surveillance cameras are installed, all have fixed fields of view. A Software House intrusion detection arming station and fire alarm pull station are obstructed by the television placement.</p>	<p>Security electronics is well deployed, consideration of multi-sensor or dual-head cameras would have enhanced video coverage using the same infrastructure installed for fixed field of view cameras.</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
100		<p>VRC offices are all equipped with access control measures. There are no window treatments installed on the interior glazing, but they are available on exterior facing glass. Ability to secure themselves and hide in a lockdown is challenging for office occupants.</p>	<p>Consider installation of dropdown window treatments or application of frosted film to restrict visibility onto the offices in the event of shelter-in-place or lockdown.</p>	3
101		<p>The Data Room is access controlled. There are three cameras within this small space monitoring all activity, this is overkill in comparison to much larger data rooms across the district with no video surveillance deployed. A Software House access control enclosure and power supplies are wall mounted. An American Dynamics video surveillance local network video recorder is rack mounted. The card readers used at the building are HID Multiclass which support several different credential types.</p>	<p>Installation of three cameras is overkill and inconsistent with any other data room on campus. 24 VDC power transformers should be housed within a security enclosure to avoid potential tampering with.</p>	0





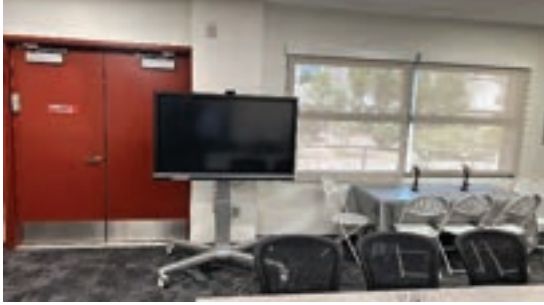
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
102		<p>STEM Center Rm. 115 is a classroom that houses expensive equipment. The door is not locked from the exterior side providing free ingress to all building users. The door appears not to be in the path of egress and has no exit sign installed above it. The ATM and vending machine have a Vivotek video surveillance camera installed monitoring activity, there is signage also indicating that there is video surveillance monitoring all activity. The cameras are believed to be non-operational with no onsite visibility of video available.</p>	<p>Rm. 115 should be secured, and general access restricted to controlled entry by card reader or brass key. Replacement and/or removal of the video surveillance cameras is recommended if non-operational. There is potential liability impact if cameras and signage are installed but the system non-operational or monitored as indicated. A standardized approach to video solution used, edge devices installed, and system administration is recommended.</p>	3


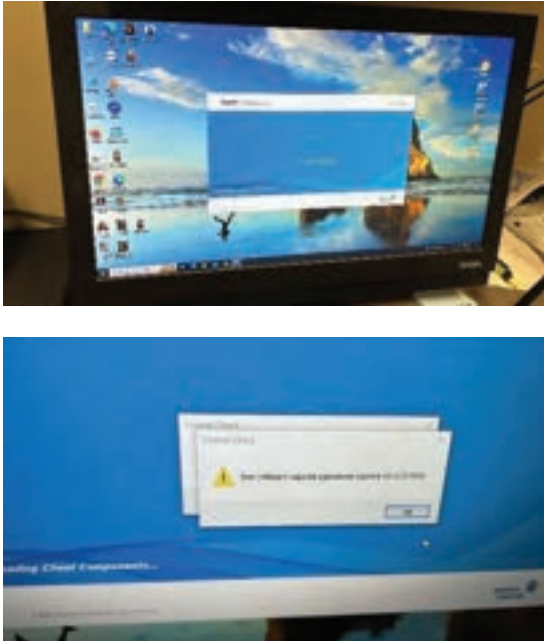
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
103	  	<p>The STEM Building has an intrusion system with Bosch arming station located within the main entry lobby. Video surveillance cameras are well deployed across the entire space however it is assumed that many of them are not operational. As with observation #102 signage indicates that there is video surveillance monitoring all activity. This is incorrect information if the video surveillance system is not operational.</p>	<p>Reference recommendation #102.</p>	3
104		<p>STEM Buildings 200 and 300 were former early childhood learning center space and have 6' chain-link fencing providing delineation of the perimeter on two sides. Classroom 302 is accessible by brass key only. There is no access control or video surveillance in use. Windows have blinds installed</p>	<p>Existing security measures are appropriate, implement future security measures upgrade subject to any future security standards that may be created to provided minimum baseline conditions across all district campuses.</p>	2

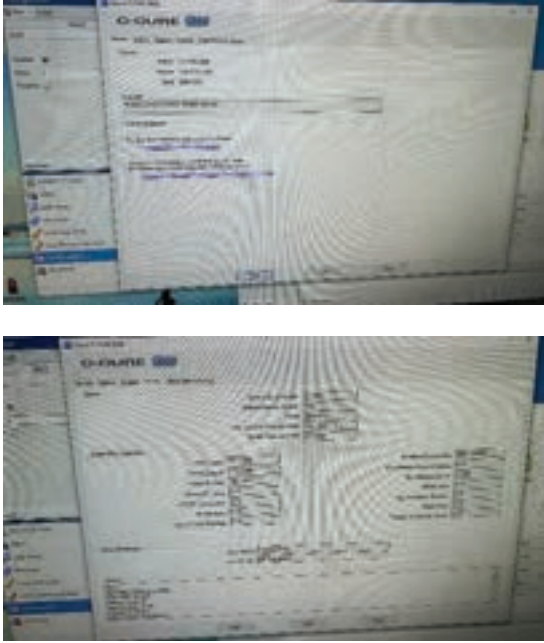
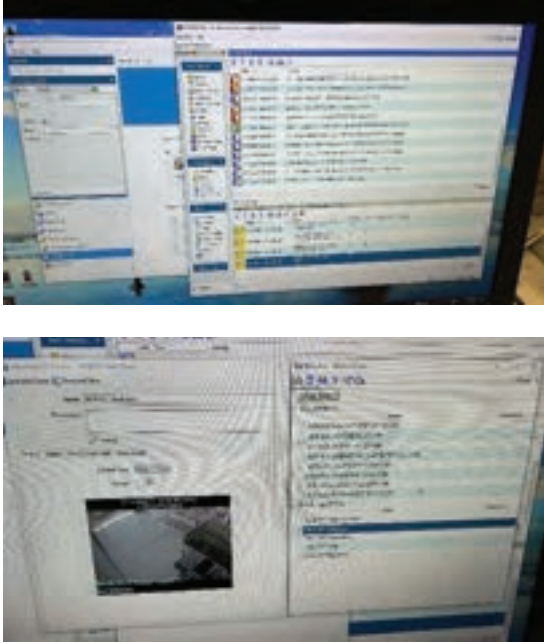
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
	 <p>The first photo shows an outdoor paved area with a tree and a building in the background. The second photo shows an interior room with a red door, an 'EXIT' sign, and various notices on the wall. The third photo shows a classroom with several tables and chairs. The fourth photo shows a close-up of a keypad mounted on a wall next to an 'EXIT' sign.</p>	<p>that can reduce visibility when turned. A Bosch intrusion detection system arming keypad is located within the food pantry, along with a telephone.</p>		
105	 <p>The photo shows a road intersection with a set of bollards in the foreground. There are trees and buildings in the background under a clear sky.</p>	<p>Third Street bollards are rollover style and intended to function as a deterrent to lane crossing rather than stop vehicles. There are concerns with traffic management at this location with speed issues a challenge. Lack of speed cushions, supporting speed restriction signage, video surveillance and offset lights fail to support</p>	<p>Perform a traffic program review of this area with a qualified traffic consultant. Adjust the existing offset lights so that vehicles can clearly observe upon approach. Consider speed cushions to reduce vehicle speeds and a raised crosswalk that require all vehicles to slow on approach of the crosswalk. Application of</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>positive speed management. VRC staff expressed concerns with near misses frequently occurring.</p>	<p>tarmac painted signage would provide visual notification of the crosswalk, with signage deployed from a distance providing early notification. Deploy video surveillance cameras to support forensic viewing and function as a deterrent to speeding vehicles, use appropriate signage to communicate that cameras are in use.</p>	<p></p>
<p>106</p>		<p>The Operations Center (OC) is unlocked and freely accessible during normal hours of business. After-hours the yard and office are secured, there is continual presence of staff in the area providing eyes on activity throughout the day. Access controlled spaces are opened during the day to provide efficiency of access as needed and to support air flow as no HVAC within the work bays. Trash dumpsters are positioned within dedicated gated spaces.</p>	<p>General observation, the significant amount of activity that occurs during the normal hours of operation provides extensive eyes-on-activity. Maintaining closed and secured work bays at all times is impractical and would impede operations. People activity and ownership of the security program is key to maintaining a safe environment at the OC. Video surveillance does support situational awareness and forensic viewing.</p>	<p>0</p>

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
107		<p>OC 157 houses all the brass key cutting machinery etc., access to this is restricted to brass key with no access control measures applied. The restricted access is limited to one or two keys. There are issues related to limited key distribution if in the event of an emergency neither key holder is onsite.</p>	<p>Recommend that this room be controlled access via a security credential, video surveillance of the opening should be interfaced with access control. This room contains sensitive materials and tools that are critical to the campus security program, ability to audit check access should be available. Limited brass key issuance may have negative implications if an employee with brass key access to the space leaves employment and keys are not returned.</p>	4
108		<p>The OC Network Operation Center houses a workstation that is used to program the entire campus DMP intrusion detection system. All office doors within the NOC, OC general space are access controlled. Software House access control door control modules are installed above each controlled opening.</p>	<p>Recommend that the security electronics systems be managed and administered from a central location. An integrated solution would provide maximization of investment and allow the security electronics to better serve the security program acting as a force multiplier to existing stretched security staffing levels.</p>	3

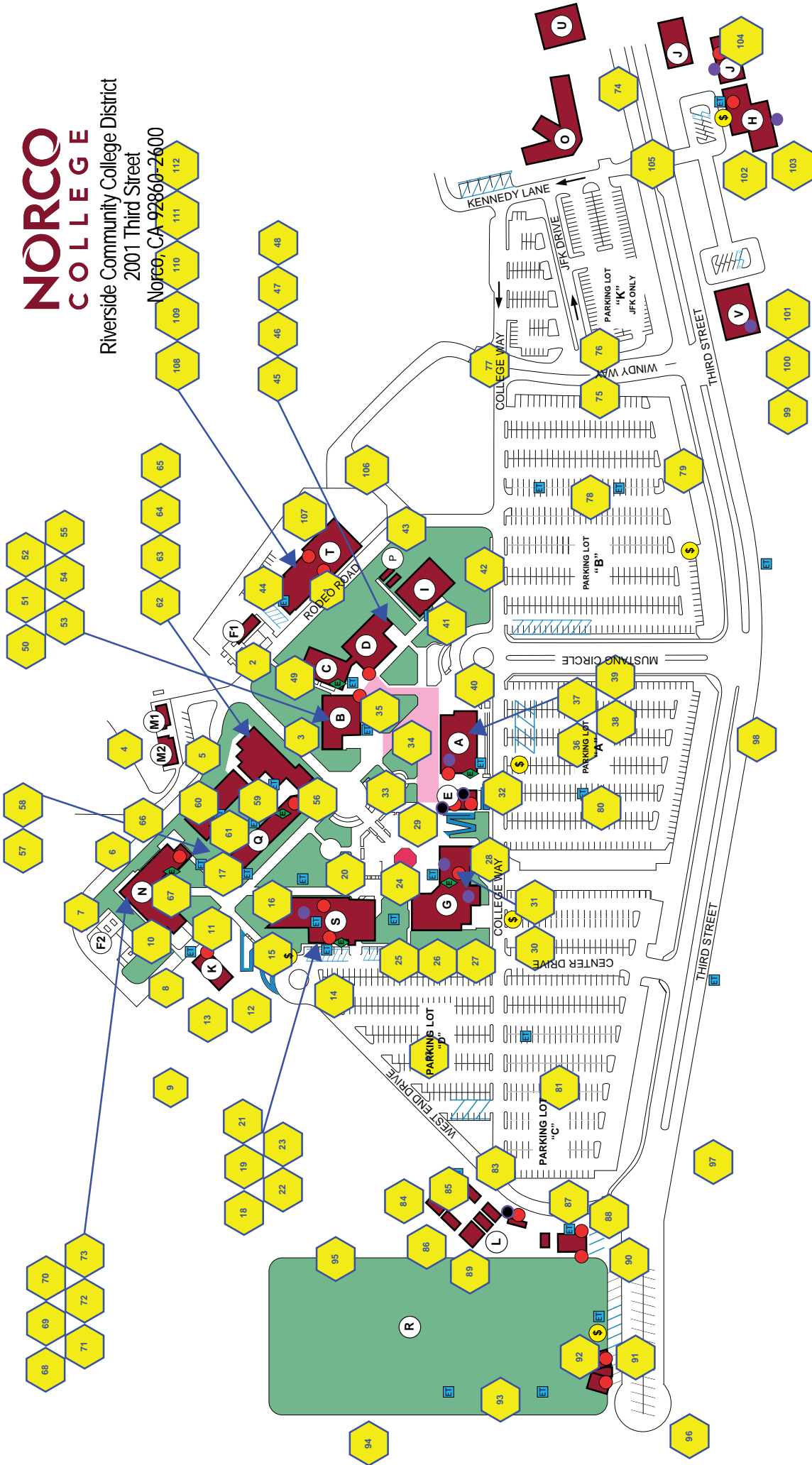
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
109	   	<p>A POTS landline is located in the designated EOC space. Every campus has a POTS line; however, this is the first campus where we have physically observed the red handset. The number displayed was tested and is still operational. Radios and emergency EOC equipment is stored within the cabinets. Role specific laptops are set-up ready for use if needed.</p>	<p>Measures in place are excellent, the district should conduct a frequent testing and validation of emergency POTS lines at all campus locations.</p>	0

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
110	 <p>The first photo shows a white HID iClass security card with a QR code and text. The second photo shows a workstation with a monitor, keyboard, mouse, and a camera on a tripod. The third photo shows a grey security panel with a white label.</p>	<p>The college is using HID iClass security card credentials, these are 13.56 MHz contactless cards, user photo image can be applied to the cards on issue. The workstation provides visibility of the Software House access control and video surveillance systems, network connection appeared slow.</p>	<p>Use of higher frequency encrypted security credentials is excellent and should be used across all district facilities, 125 kHz frequency should not be used. Reference recommendation #108 regarding security electronics systems management and administration. Security credentials across the district should contain photo imaging of the credential holder, there is inconsistency in this approach across the district.</p>	3
111	 <p>The first photo shows a computer monitor displaying a desktop with a blue background and a white pop-up alert window. The second photo is a close-up of the alert window, which contains text about an expired software support agreement.</p>	<p>A pop-up alert advised that the CCURE 9000 software support agreement expired on 3/31/2024. Each college campus is responsible for maintaining their own SSA's, this is inefficient and results in security technology being under used and failing to provide benefit of investment if SSA's are allowed to expire. We understand that the same local responsibility regarding camera licenses also applies. CCURE version 2.90 is operational.</p>	<p>Recommend that the district review the security electronics systems ownership and funding model currently used. Consider a centralized systems management and ownership approach with local support administrators. The current local ownership and funding model impacts the entire district security culture and presence, as there is inconsistency in use and expired SSA's and licenses renders equipment invested in redundant.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
112		<p>Alarm events are not monitored, managed, or responded to. American Dynamics network video recorders were identified and cameras able to be called up. There is no programmed interface between any existing security electronics system at Norco College or any other campus.</p>	<p>Reference recommendation #111. Develop security standards that provide minimum baseline expectations of security electronics installation across district facilities by built environment type. Integrate security electronics using open-source systems to enhance technology capability to act as a force-multiplier to existing security and police staffing levels.</p>	3

NORCO COLLEGE

Riverside Community College District
2001 Third Street
Norco, CA 92860-2600




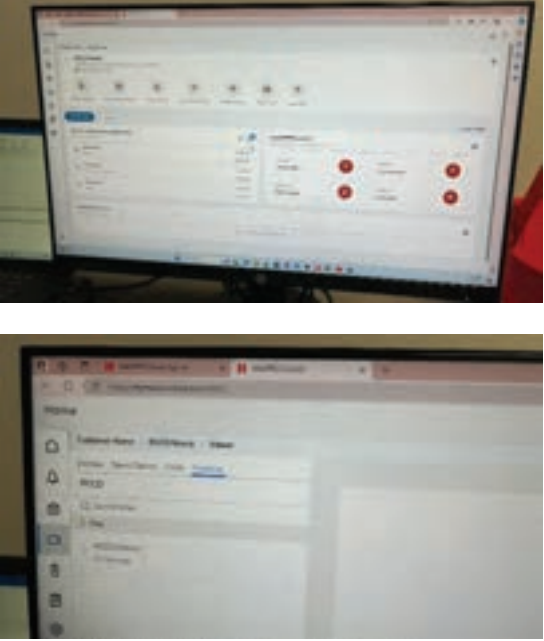


- A Student Services - (SSV)
- B Science & Technology - (ST)
- C Theater - (THTR)
- D Humanities - (HUM)
- E College Safety and Police
- F College Resource Center
- G Central Plants
- H Wilfred J. Airey Library - (LIBR)
- I STEM Center 100
- J Bookstore
- K STEM Center 200 & 300
- L Center for Applied and Competitive Technologies (CACT)
- M West End Quad - (WEQ)
- N Facilities
- O Applied Technology - (ATEC)
- P John F. Kennedy Middle College High School (JFK)
- Q Portables A & B (Faculty Offices)
- R Industrial Technology (IT)
- S Sports Complex
- T Brenda and William Davis Center for Student Success (CSS)
- U The Corral (Cafeteria and Dining Room)
- V Operations Center (OC)
- W Center for Workforce Innovation (CWI) Norco Business Park
- X Veterans Resource Center (VRC)



- Elevators
- Restrooms
- Disabled Parking
- Amphitheater
- Emergency Phones
- Parking Pay Station
- Free Speech Area
- Gender neutral restroom
- Student neutral restroom
- Faculty



	Elevators		Amphitheater
	Restrooms		Emergency Phones
	Disabled Parking		Parking Pay Station
	Disabled Ramps		Free Speech Area
	One Way Road		Gender neutral restroom
			Student neutral restroom
			Faculty


Norco Innovation Center

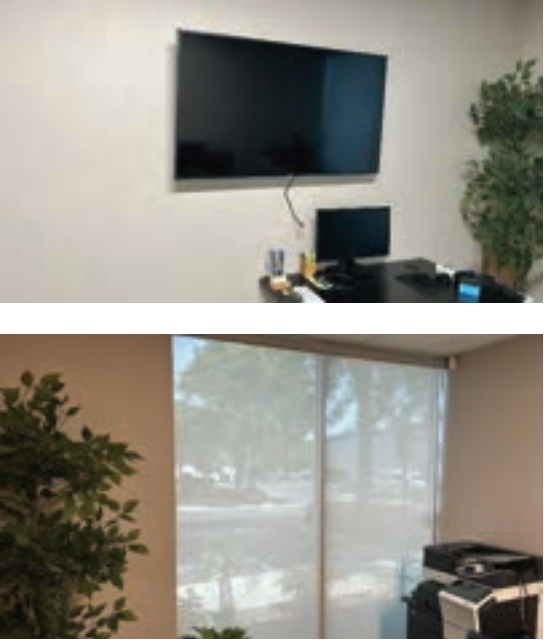


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>All security access control devices and video surveillance cameras are Honeywell product and system. This is a legacy existing tenant system who were previously the owners of the building. Access to the access control application is provided to the district allowing for activation and deactivation of security credentials. District cannot view video surveillance cameras locally; it is assumed that district police can monitor cameras. The tenant holding control over a security system that includes shell devices is unusual.</p>	<p>Replace the existing security electronics systems with district owned and managed systems. The tenant should not have visibility of cameras outside of their leased space without written authorization from the district and confirmation by legal counsel that there is no liability impact on providing access. The assumption that district police can view video surveillance cameras appears incorrect. Verify if district police can or cannot view video cameras and confirm if they do require viewing rights. Security electronics system standards should be created, and systems interfaced.</p>	4

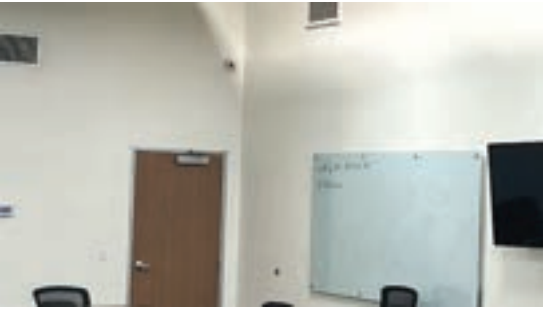
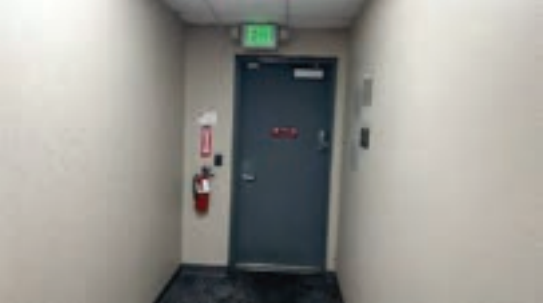
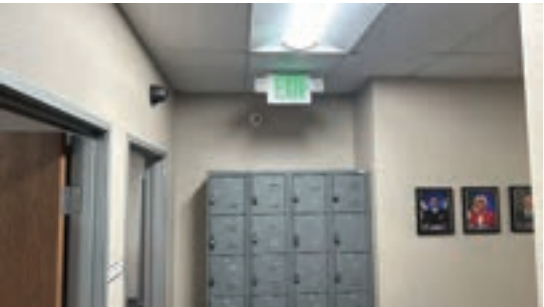
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>District staff member has access to the Honeywell access control cloud portal and can provide permissions to security credentials to access specific openings. The administrator does not actively receive alarm events, the system is not used to proactively support security operations.</p>	<p>Consider creation of a districtwide security operations center (SOC) to manage access control system alarm events. The current security program locally and across the district lacks management of the security electronics systems, alarm events are not proactively used to support management of, or response to alarm events. Investment in security technology is not maximized.</p>	3
3		<p>HID ProxCard II are issued to both district and tenant employees. The tenant informs the district administrator when an employee left employment so that credentials are deactivated. The district staff are unsure of how many brass keys are in circulation providing entry to the building. The tenant has not shared any key issuance records with the district.</p>	<p>Perform a review of the building keying status, consider rekeying the exterior locks with new key cylinders and controlled brass key distribution. Distribution of keys should be minimal with access control credentials the primary access tool. The district should migrate away from Prox cards that can easily be copied.</p>	4
4		<p>Exterior accessible access control and intrusion detection equipment is located within the electrical room. The electrical room is accessible by brass key only. There is no video surveillance camera monitoring the equipment or drip tray installed under the HVAC unit. Battery back-up should be</p>	<p>The electrical room should be controlled with card reader providing an audit trail of approved access or unapproved entry attempts. A video surveillance camera should be installed internal to the space providing deterrent and visibility of activity. Best practice is to remove keys from the security</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>replaced with new as existing is approximately 3-years old. Keys to security enclosures should be removed.</p>	<p>enclosures to prevent potential tampering by unauthorized persons, batteries should be replaced on schedule every 2 to 3 years. If the HVAC system is not plumbed, install a drip tray. Security electronics system standards should be created, and systems interfaced.</p>	
5		<p>The intrusion detection system also utilizes Honeywell product. There is no integration between any of the security electronics which are all Honeywell products. Security electronics is not providing operational benefit to building safety and security. Power supplies are powered by cable plugged into a receptacle.</p>	<p>Security electronics system standards should be created, and systems interfaced. Recommended migrating to the DMP intrusion system used consistently across district facilities. Best practice security electronics installation is to hard wire security power or house power transformers within security junction boxes/enclosures.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
6		<p>An exterior video surveillance camera monitors general activity in the vicinity of the electrical room. Access into the electrical room requires a brass key, there is no access control applied to restrict unauthorized access into this space.</p>	<p>Reference recommendation #4, the video surveillance camera if lowered to approx. 10' AFF would provide visual coverage of the electrical room point of entry. Interface with the access control and intrusion detection systems.</p>	3
7		<p>Glazing has reflective measures applied to it, reducing visibility from the exterior side during the hours of daylight. There are no ballistic treatments applied to the glazing. There is a single video surveillance camera located on the ceiling, providing situational awareness of activity at the main point of entry. There</p>	<p>Consider a video intercom at the main entry providing ability to communicate with persons requesting entry visually and audibly if the building. This eliminates the risk associated with having to open the door to verify why someone is requesting entry if not an authorized security credential</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>is no video intercom installed allowing for two-way audible and visual communication with persons seeking entry prior to granting it.</p>	<p>holder. Consider use of industry standard ballistic level protection rating at exterior doors and windows that may require ballistic-level protection.</p>	
8		<p>The district office spaces are accessible by brass key only, there are no electronic access control measures. Both doors can be locked from the interior using a thumb turn, door closers are not installed, and neither were lock bloks.</p>	<p>Install lock bloks and door closers to support positive latching upon closure. Doors should always function in a locked state. Installation of access control at these offices should be considered as the district staff do not occupy them each day and the tenant has access to the space directly outside the offices. Install a multi-sensor camera in the reception area monitoring general activity.</p>	3
9		<p>District offices do not have desk mount telephones provided, this is inconsistent with other office and administration locations across campus. The monitor on the wall would be ideal for live streaming of video surveillance camera activity.</p>	<p>Provide VoIP telephones in all district offices, consider live stream of video surveillance cameras on the monitor. Reference recommendation #1 regarding video surveillance ownership.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
10		<p>Exit opening has a local door alarm installed and has a spy hole providing visibility of exterior activity. The door has an internal locking lever. The external roller shutter door has been framed in.</p>	<p>Replace all battery local alarms with hard wired, eliminate potential lack of power monitoring and battery replacement issues that standalone and wireless devices present.</p>	2
11		<p>The local door alarm is non-operational, an intrusion detection arming station is located on the wall. Unique arming/disarming codes are issued to district staff and to the tenant, there is uncertainty regarding the tenant management of codes. There are two video surveillance cameras in this conference room, and the interior card reader was a leftover from the tenant when owner who used the interior card reader to monitor their staff presence.</p>	<p>Remove legacy internal card readers previously installed for prior building owners' management of people attendance. Repurpose or install new card reader that is used to arm and disarm the intrusion detection system, eliminate use of arming station codes that can be shared. Replace all battery local alarms with hard wired, eliminate potential lack of power monitoring and battery replacement issues that standalone and wireless devices present.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
12		<p>Internal card reader installed on the interior of the corridor exit was used by the now tenant when they were the previous owner as a means of performing an audit check when staff were entering and exiting the building. The internal card reader does not unlock the door as free egress is always available, the card readers are now redundant. The door sounder is not operational.</p>	<p>Replace all battery local alarms with hard wired, eliminate potential lack of power monitoring and battery replacement issues that standalone and wireless devices present. Remove legacy internal card readers previously installed for prior building owners' management of people attendance.</p>	3
13		<p>Internal video surveillance cameras monitor activity within the internal corridors. Video stream is not available to the district staff on site, the tenant has control of the video storage parameters which were unknown to district staff.</p>	<p>Replace the existing security electronics systems with district owned and managed systems. The tenant should not have visibility of cameras outside of their leased space without written authorization from the district and confirmation by legal counsel that there is no liability impact on providing access. The assumption that district police can view video surveillance cameras appears incorrect. Verify if district police can or cannot view video cameras and confirm if they do require viewing rights. Security electronics system standards should be created, and systems interfaced.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
14		<p>The conference room is a shared space and requires the tenant to book the space in advance with the district staff if wishing to use. There are no access controls that restrict any access into the space if district staff are not onsite.</p>	<p>General observation only, ensure that there are no district intellectual property items stored within the room and monitor network ports to avoid potential misuse and cyber threat.</p>	0
15		<p>Window treatments are installed at the main entrance restricting visibility from the exterior public side in, there is no treatment on the door itself which is a vulnerability. There is no ability to communicate with persons on the public side prior to opening the door. There is no video monitor that live streams exterior cameras providing situational awareness in the lobby. Single occupancy restrooms have privacy indicators installed, a single camera monitors corridor activity.</p>	<p>Consider a video intercom at the main entry providing ability to communicate with persons requesting entry visually and audibly if the building. This eliminates the risk associated with having to open the door to verify why someone is requesting entry if not an authorized security credential holder. Consider use of industry standard ballistic level protection rating at exterior doors and windows that may require ballistic-level protection.</p>	3
16		<p>The wall space adjacent to the district office wall displays emergency evacuation plans, emergency procedures distributed by the district. The tenant has their own emergency evacuation plans etc.; these are not shared by the tenant with the district staff that occupy the space.</p>	<p>Coordinate with the tenant and establish a building emergency evacuation plan with procedures that are visible and understood by all building users. The district could mandate within the tenant contract that an emergency evacuation plan be provided for district review, or that the district plan is shared and followed. Do not operate with two different plans and procedures within such a small space which could cause confusion and chaos if an emergency incident were to occur.</p>	4


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
17		<p>Exterior video surveillance cameras are positioned on each corner of the building. Rear access doors are equipped with access control card readers.</p>	<p>General observation only, future security electronics systems should interface to support camera call-up upon alarm event activation.</p>	0

Riverside City College

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
1		<p>South-east corner of campus off Olivewood Ave. rain channel has been known as an area where vagrants have congregated within. Open campus provides unrestricted access onto campus property as no fence line restricts access from the channel onto RCC campus.</p>	<p>General observation. Applying fencing would not impact accessibility onto campus which is open from several other areas.</p>	0
2		<p>Campus lighting uses LED luminaires maximizing lighting performance with power efficiency. The lighting in the parking lot has cut off light head fixtures. The downwards distribution of lighting reduces light pollution and provides good color rendition. There is no emergency phone located in this parking lot. Video surveillance cameras are typically not installed across the RCC campus parking lot areas.</p>	<p>Install electronic surveillance in parking lot locations that provide a view of the immediate area, specifically activity at primary exits and entrances. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.). Consider use of license plate recognition video cameras.</p>	2
3		<p>General landscaping at the south-east campus entry is well maintained and visibility of activity on the public sidewalks and roads is unrestricted. Tree canopies are typically above 6' in height, shrubbery is above the CPTED guideline of 2', but is managed and hiding areas minimized due to the excellent maintenance activity that occurs. Instructional and directional signage appears weathered in many locations across, and in need of a refresh either by repair or replacement. The open campus has no perimeter control measures to restrict both pedestrians and vehicles access. There is no license plate</p>	<p>Ensure all site signage is durable against human tampering and natural weather events. Post signage on the perimeter of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.). Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.). Consider use of license plate recognition video cameras.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		recognition camera capability at any vehicle entry point.	Maintain landscaping that meets CPTED guidelines.	
4		Utilities mains are not protected with any protective caging. Access to the turn controls is restricted with a chain-link and padlock however, this can easily be cut. A-frame signage providing directions for student and visitor were observed at the four-way intersection. On campus street signs use campus colors, which are orange text on a brown background. This is difficult to read when approaching in a vehicle as are signs with small text that provide rules and regulatory code measures that support consequence for potential not following. General signage and wayfinding application is poor.	Ensure all site signage is durable against human tampering and natural weather events. Post fixed signage on both the perimeter and inner areas of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.). Design text and finishes on signs for clarity and ease of reading. Consider additional security measures of the utilities by applying a cage, review any issues with cold that may restrict additional security measures being applied.	3
5		Campus landscaping is well-maintained with setback space between sidewalks and buildings at least 6'. Landscaping on the facilities building perimeter does not restrict visibility and clear lines of sight from within the building looking outwards are excellent. The majority of building windows have window blinds lowered and drawn eliminating visibility of activity.	Maintain landscaping to be a physical barrier for the building and obstruct view angles (take care not to create hiding places), but not to obstruct the lines of sight to see pedestrians or vehicles approaching the building. Utilize landscaping and other site features to provide for effective surveillance and reduce opportunities for concealment or entry into the facility. Existing use of the window treatments is appropriate.	0
6		Perimeter fencing at the facilities yard is 6' in height and easily scalable, screening is applied to restrict visibility of items stored within the yard. This does not provide any deterrent to persons with intent to cause harm or take items left accessible. In addition to the height of the fence, a person can slide under the gates as they do not reach the ground and the gap is extensive enough to crawl under. A Verkada video surveillance camera is installed	Review fencing height and develop a standard with minimum fencing height of 7', use of fence toppers may also provide deterrent to unauthorized scaling. Review the vulnerability presented by the gate height and eliminate the ability for crawling under. Ensure all site signage is durable against human tampering and natural weather events.	3

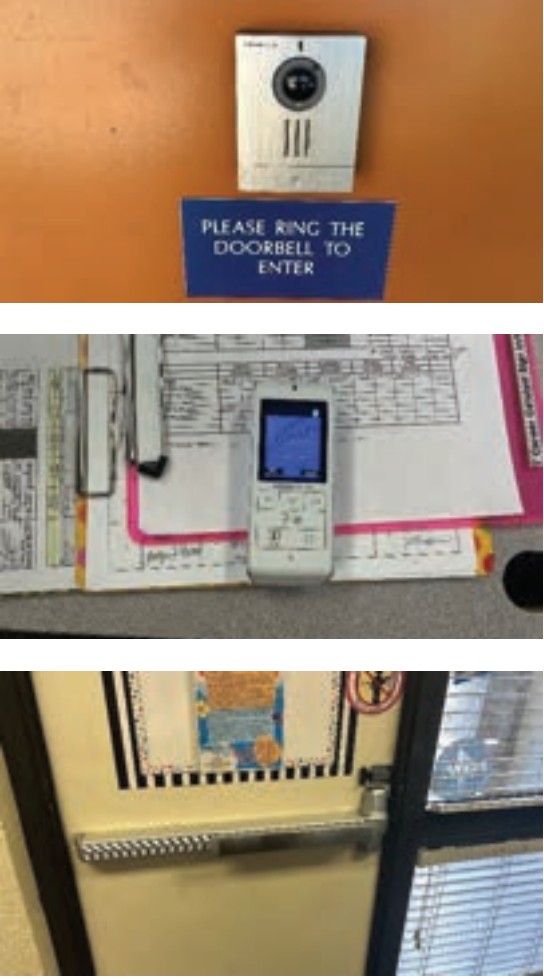

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>monitoring activity at the vehicle entry gate. Instructional and rule enforcing signage around the campus in many cases is weathered and in need of repair.</p>		
7		<p>Tennis courts are freely accessible at all times and visibility in is restricted with screens. Courts are used by the community and remain unlocked at all times. There is no video surveillance coverage of any activity both at the exterior and interior of the tennis court areas. There is no emergency phone located adjacent to the tennis courts on the Saunders St. side.</p>	<p>Install electronic surveillance in tennis court locations that provide a view of the immediate area, specifically activity at primary exits and entrances. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.). Consider locking and unlocking the tennis court and schedule to restrict unauthorized use and access. Consider installation of emergency phone towers on both sides of the tennis courts.</p>	2
8		<p>Area at the rear of the gymnasium is open and nefarious activity is known to occur here. The perimeter fence line is damaged and provides unrestricted access from the adjacent property in. Video surveillance is not installed at this area providing no monitoring of activity forensically.</p>	<p>Review fencing height and develop a standard with minimum fencing height of 7', use of fence toppers may also provide deterrent to unauthorized scaling. Create security design standards that deliver governance be guarding application of security electronics and physical</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>measures to both sites and buildings dependent upon use. Install electronic surveillance that provides a view of the immediate area. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc.</p>	
9		<p>Staff parking Lot V lighting is provided by two spotlights that are positioned adjacent to a tree. The tree should be trimmed regularly to ensure that the lighting is not obstructed by overgrowth.</p>	<p>Prioritize maintenance and repair that could affect the security of facilities such as parking lot lighting. Install electronic surveillance in parking lot locations that provide a view of the immediate area, specifically activity at primary exits and entrances. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.). Consider use of license plate recognition video cameras.</p>	3
10		<p>Tagging on campus is a frequent occurrence and had been applied to the one-way sign at the perimeter road adjacent to the swimming pool.</p>	<p>Prioritize maintenance and repair that could affect the perception of safety and security of facilities such as removal of graffiti/tagging from signage.</p>	2
11		<p>Swimming pool perimeter fence line is easily scalable. There is no video surveillance monitoring any of the activity at the swimming pool area which presents potential liability issues if an incident were to occur. Ease of access into the swimming pool is concerning. A Code Blue emergency telephone was</p>	<p>Develop security standards including review of fencing heights and material. Consider future use of decorative fencing that does not have flat top rail to support ease of scaling. Unauthorized activity at the aquatic center carries significant risk and liability to the college that should be mitigated. Video</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		observed mounted to the wall in the swimming pool area, lack of video surveillance does not support camera call-up upon activation of a call.	surveillance should be installed both on the perimeter and the inner pool deck areas to provide both situational awareness and forensic video review capability.	
12		Emergency tower phone communication is wireless, the blue strobe is not illuminated at all times; and the face plate of the emergency phone unit is completely weathered and the signage on the face plate no longer legible. The emergency tower was originally red in color but is extremely old and is not easily identifiable for a distance. At night, the emergency phone is illuminated by the adjacent LED light. Emergency phone towers/casing should be vibrant in color for ease of identification.	Implements an upgrade program that addresses all of the emergency phone towers on campus. Create an operational standard that support consistency in device type application. Replace all end of life and non-operational emergency call stations with new. All call stations that are currently out of operation should be bagged and signage provided that indicates that the unit is out of order.	4
13		The narrow bridge has weight restrictions displayed on signage, but access is unrestricted. The landscaping is well-maintained and areas of concealment for bad actors is minimal. Old posts appear damaged and have not been removed, lack of maintenance/repair does not impart a positive impression to campus visitors.	Consider removing all redundant security measures that do not present a positive impression big adding the campus security posture. Install vehicle barriers that provide compartmentalization of the campus to authorized vehicle access only.	1
14		Delineation between campus property and adjacent land is poorly identified with district property rolling into others. Campus entry points lack bold celebrational signage that broadcasts that persons are entering college grounds. The hospital staff parking lot adjacent to the rear of the early child education center provides unrestricted visibility from an elevated vantage point into the facilities play area. This unrestricted visibility presents significant risk that requires mitigating. The open nature of the campus perimeter allows opportunity ease of scaling the	Ensure all site signage is durable against human tampering and natural weather events. Post fixed signage on both the perimeter and inner areas of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.). Design text and finishes on signs for clarity and ease of reading. Review the campus perimeter and consider installation of an 8' chain link fence with visibility slats to restrict observation of the play area from the public side of the campus. Video surveillance should be installed to provide	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>fence line at the bottom of the hill. There is a lack of way finding signage across the campus that supports ease of identification of current location. Additional signage indicating the direction of campus buildings is missing at this entry from 15th St.</p>	<p>situational awareness and forensic video review capability.</p>	
15	   	<p>The unrestricted visibility from the public sidewalk into the play area from Magnolia Ave. presents risk to the ECEC occupants, and opportunity for vagrants and unhoused to use the facilities for their own benefit due to ease of access. Misuse and unauthorized use of the exterior facilities by the unhoused, results in staff checking the play area daily for leftover remnants of drug abuse including needles etc. Readily available cleaning supplies within the play area including hand and other cleaning materials, access to water via the drinking fountains, and plenty areas of cover that provide shade, make an ideal area for misuse by unhoused. There is no video surveillance installed that provides real-time situational awareness viewing capability or option to review activity forensically.</p>	<p>Refer to recommendation #14, perform maintenance corrections to the existing chain-link fence line.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
16		<p>The fence line at the parking lot of the ECEC is 6' chain-link and is damaged at many points. Signage is also weathered and in need of replacement to become legible and provide governance to use of the parking lot.</p>	<p>Ensure all site signage is durable against human tampering and natural weather events. Post fixed signage on both the perimeter and inner areas of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.). Perform maintenance corrections to the existing chain-link fence line.</p>	3
17		<p>The perimeter fencing that is installed within the ECEC area leading to the rear play area is inconsistent in height and easily scalable. The inconsistency in height provides opportunity for bad actors to simply step over the fencing using the existing retaining wall as leverage. Again, the lack of video surveillance fails to support operational efforts to maintain safety and security of the most vulnerable people on campus.</p>	<p>Review fencing height and develop a standard with minimum fencing height of 7', use of fence toppers may also provide deterrent to unauthorized scaling. Install exterior video surveillance.</p>	4
18		<p>Access to the ECEC office is via activation of a video intercom, with entry provided from the interior via pressing of a momentary remote release button. The door remains closed and locked during normal hours of operation, unless approved entry is provided following verification of visitors using the</p>	<p>Supplement the existing portable video intercom unit with fixed video master stations that provide remote release directly using the handset. Install video surveillance on the exterior of the opening to provide situational awareness and forensic video review capability. Install a viewing monitor within</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>video intercom. There is no video surveillance that provides the ability to monitor activity occurring on the exterior of the building or directly outside the main point of entry.</p>	<p>the office space providing visibility of exterior activity in real time. The current operation of the door remaining closed and locked during normal business hours is appropriate.</p>	
19		<p>Exterior restrooms are completely unlocked and provide opportunity for any person to loiter inside with intent to cause harm. Again, the lack of video surveillance does not allow for situational awareness visibility of activity within the restroom vestibule area, or ability to monitor activity on the immediate exterior of the building both in real-time and forensically.</p>	<p>Install electronic surveillance that provides a view of the immediate area, specifically activity at primary exits and entrances. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.). Consider locking and unlocking the restrooms on schedule or provide staff key access to restrict unauthorized use and access.</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
20		<p>The access point into campus from Ramona Drive is well-maintained with exceptional landscaping maintenance reducing potential areas of concealment, and lines of site below 6' kept unobstructed. Signage clearly identifies that parking permit are required. Signage is used to reinforce rules with new signage indicating that firearms are not allowed on campus recently installed. Parking lot names and permitted use are also identified. There is no large signage on the perimeter that indicates that this is a main entry into campus. There is no video surveillance monitoring both pedestrian and vehicle activity, monitoring of vehicle license plates does not occur.</p>	<p>Install electronic surveillance in parking lot and vehicle entry locations that provide a view of the immediate area, specifically activity at primary exits and entrances. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.). Consider use of license plate recognition video cameras. Consider installation of large signage that clearly indicates that this is a main entry into campus and showcases and celebrates the campus.</p>	3
21		<p>Parking lot lighting is restricted to the perimeter of the parking lot area, this appears sufficient for the small area. Tarmac markings are weathered and in need of repainting to reaffirm the parking bays and ADA parking areas etc.</p>	<p>Performed maintenance activity to reinforce the painting on the tarmac that identifies the parking bays and permitted use. Install signage that is durable against human tampering and natural weather events. Post fixed signage on both the perimeter and inner areas of the facility that denotes site perimeter or specific instructions (e.g., no trespassing, restricted access, site is monitored, no parking, etc.).</p>	3
22		<p>The Code Blue emergency phone tower is currently out of service due to construction in the adjacent parking lot. The Code Blue call stations are hardwired and have blue strobes mounted at the top. The lack of video surveillance deployment on campus fails to support ability for camera call-up to occur when a call is placed.</p>	<p>Apply signage that clearly indicates that the emergency phone tower is currently out of order. Consider a security standard that deploys video surveillance either adjacent to all emergency phone stations or is incorporated into emergency phone towers, providing situational awareness upon activation of the call station.</p>	5


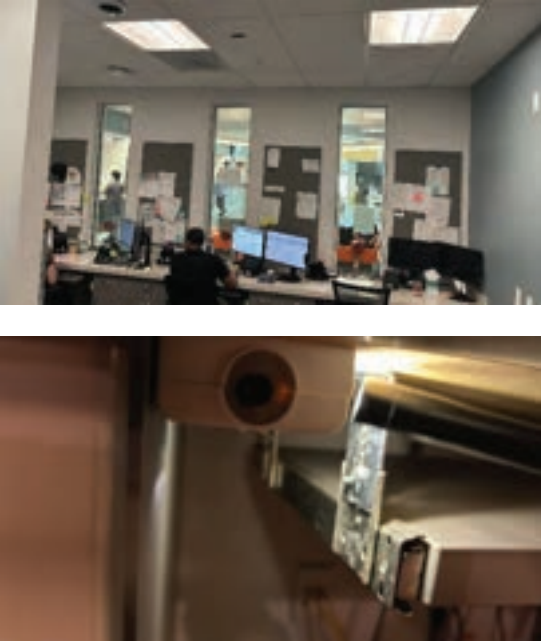

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
23		<p>The Main Administration Office exterior windows are equipped with window blinds that restrict visibility into the space from the public side. The cashier's office glazing has ballistic film which has been applied post glazing installation. Access control is applied to exterior doors and a video intercom is used at the exterior cashier's office for remote release entry to be provided from the interior. Lighting on the exterior of the building and on the adjacent sidewalk is extensive. There is no exterior video surveillance monitoring the controlled entry points or the general area.</p>	<p>Install exterior video surveillance providing visibility of all activity at controlled and monitored points of entry or egress. Use industry standard ballistic level protection rating film at exterior windows and glazed doors that require ballistic-level protection. Develop a security standard that identifies windows and door locations that would require ballistic level protection.</p>	3
24		<p>Clear delineation of public sidewalk and campus property is achieved with excellent maintained landscaping. The setback clearly defines public and district property.</p>	<p>General observation.</p>	0
25		<p>Video surveillance cameras are installed in many locations across the campus however they are non-operational. There are several disparate standalone video surveillance systems installed and none of them are centrally managed. It is unknown the number of disparate systems installed, the lack of operational state of many devices presents potential liability issue to the district if a subpoena for video was made and the district unable to provide due to cameras being non-operational. Video surveillance also can impact the security culture and "sense" of security felt by campus users. Neglect of maintaining operational state may have a significant impact on reputation,</p>	<p>Develop a security standard that identifies a single unified platform that will provide systems administration of video surveillance, access control, and intrusion detection. Provide maintenance review of all existing video surveillance cameras to identify cameras that are non-operational. Develop a phased program that will fix or replace existing cameras with new. Implement this a security electronics system administration program that utilizes the technology to better serve physical staffing measures, acting as a "force multiplier" to existing campus police presence. Technology should be used to support incident response and forensic review of incidents.</p>	2


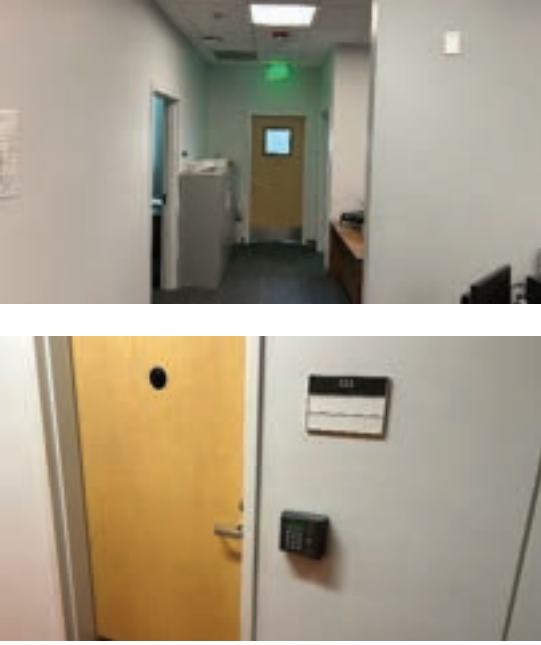
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		culture, and finances if a catastrophic incident occurs that results inability to review activity or use as part of an incident response.		
26		<p>Exterior restrooms at the Math's and Science (MTSC) building are controlled on the access control system and unlocked on schedule. In a lockdown situation the doors automatically lock with no notification and no communication capability of informing occupants that a lockdown has been activated. Vape detectors are not installed in any student/public restrooms. Mass communication across the campus is 100% reliant upon cell phone SMS messaging and RAVE mobile application push notifications for those that opt-in to the application. Public address speakers both internal and external are not present.</p>	<p>Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. The lack of communication availability to occupants within the restroom in the event of a lockdown is a liability that requires mitigating. Improve communications across campus from an information perspective providing education on the different means of receiving mass notification communications. There is misunderstanding amongst campus users, with many only aware of the RAVE mobile application communication and nothing else.</p>	4
27		<p>Wayfinding map placement across campus is sparse. It is difficult for visitors to easily orientate themselves with their position on campus or identify other buildings as the few wayfinding maps in use do not have "Here" markers in use on them. QR code digital wayfinding maps are not in use.</p>	<p>Provide additional wayfinding maps across campus at heavy foot traffic locations to help provide campus users with the ease of identifying their current location, and the location of other buildings that they may be seeking. Consider use of QR codes that provide virtual wayfinding maps that campus users can use on cell phones.</p>	3
28		<p>The seating area provides excellent natural surveillance of activity. There is no technology applied to support both visual monitoring of activity and provide communication if an incident occurs. The elevators are available for public use on schedule.</p>	<p>Install video surveillance to monitor activity in the immediate area. Consider connection of the elevators to the access control system to support remote locking and unlocking on schedule.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
29		<p>The campus entry from Magnolia Ave. and Terracina Dr. is identified by signage displayed in the perimeter wall. There is good setback from the sidewalk to the building. Video surveillance is installed on the building exterior. There are no speed bumps or speed restriction signage installed in the main entryway leading to the parking garage. Across campus there is a complete void of speed limit signage in use. The bus drop off/pick-up is set back from the sidewalk and provides complete visibility of surroundings with an open bus shelter installed. The seating bench encourages people to sit and observe activity, its design by nature restricts people from sleeping on it.</p>	<p>Design traffic patterns to ensure circulation that prevents high-speed approaches by visitors; barriers, planters, and landscaping may be useful. Install signage that clearly indicates speed limit and locations that are easily observed by vehicles entering and exiting campus.</p>	3
30		<p>Exterior entry into the classroom at the Administration Building (CAK) is via access control. The controlled exterior doors are monitored with door position contacts and there are several ceiling mount intrusion motion detectors. All exterior facing windows are equipped with window treatments (blinds) which were lowered. Intrusion</p>	<p>Develop security design standards that ensure that all exterior openings are monitored with door position monitoring contacts. Review electronic hardware and consider use of quiet electrified latch (QEL) retraction panic hardware eliminating the need for 1 AMP inrush, replacing with 24 VDC power.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>system arming stations are allocated per building and not on a per classroom basis. Corbin Russwin panic hardware is installed and requires 1 AMP inrush per the college locksmith. Request to exit motion sensors are mounted on the ceiling rather than integrated within the hardware. The single door at the rear of the classroom is not equipped with a door position monitoring contact and relies upon the ceiling mount motion detector to identify any movement within the space if access is made through this opening.</p>		
31		<p>The main entry doors into the CAK building are electrified sliders with access control, and an ADA push plate (actuator) mounted on the exterior side providing access when the building is closed. There are concerns shared that in a lockdown the door sensor automatically opens the doors when activated. An operational review of technology use and how it currently performs is required. A ceiling mount request to exit motion sensor shunts the door position contacts on activation. Video surveillance cameras installed in the lobby area are believed to be non-operational. The lack of operational cameras presents</p>	<p>Review the current operational state of the opening from the interior during a lockdown. Consider installation of an internal ADA push plate that provides free egress, removing the constant opening of the doors when the internal motion sensor is activated. Review code and AHJ requirements. Conduct a review of all video surveillance cameras and perform corrective action or replaced with new, any cameras that are non-operational.</p>	4



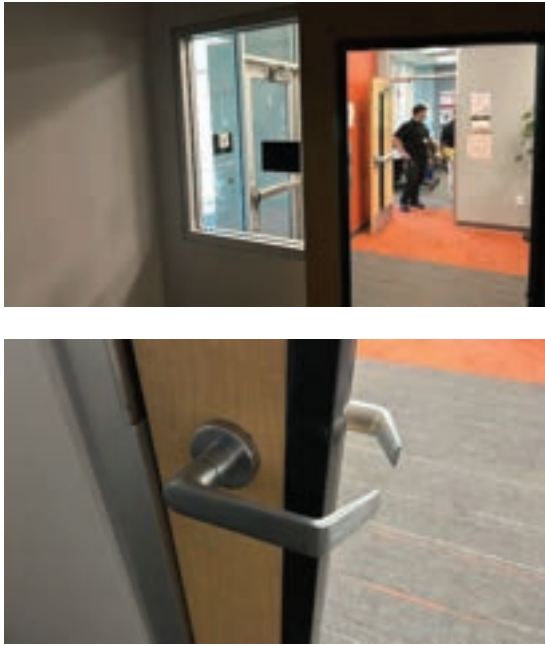
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		liability issue that requires review.		
32		Emergency procedures are distributed across campus in most buildings and are deployed by safety staff in classrooms. There distribution is excellent, and they serve as a quick reference guide for incidents including lockdown, fire, earthquake etc.	General observation.	0
33		Software House intrusion detection alarm arming stations are located in all buildings that have access control and intrusion devices installed. All non-access control buildings with intrusion devices, DMP keypad arming stations are installed. The Software House keypads are used for initiating a lockdown by input of a 4-digit code that is known by select authorized individuals.	Develop security standards that provide direction regarding minimum security requirements at each building. Review the process and protocol for activating a lockdown using the 4-digit code. Review operational considerations and alternate protocols that may reduce risk of inability to activate a lockdown if the authorized individuals are not present, determine a workaround.	3
34		Wireless panic buttons are installed under the Financial Aid transaction counter that communicate out through the access control system to the intrusion detection system monitoring station. The offsite monitoring station then alert the Riverside Sheriffs Dispatch who then notify campus police. Wireless panic buttons are reliant upon maintaining power through batteries to function as intended, the power status is not monitored on the access control system. Panic buttons are not located at every workstation which places inefficiency to activate if assistance is required at a workstation without a panic button installed. There is no physical barrier above the counter between the public and staff, the counter remains open at all times with no roller grill	Develop security design standards that provide consistency and governance to installation of devices such as panic buttons. Consider use of hardwired devices rather than wireless, wireless communication can often be impacted by the built environment; and continual review of battery life often required. Standardization of approach eliminate risk and vulnerability that ad hoc placement of devices presents. Consider installation of further video surveillance to provide monitoring of the transaction counter.	3


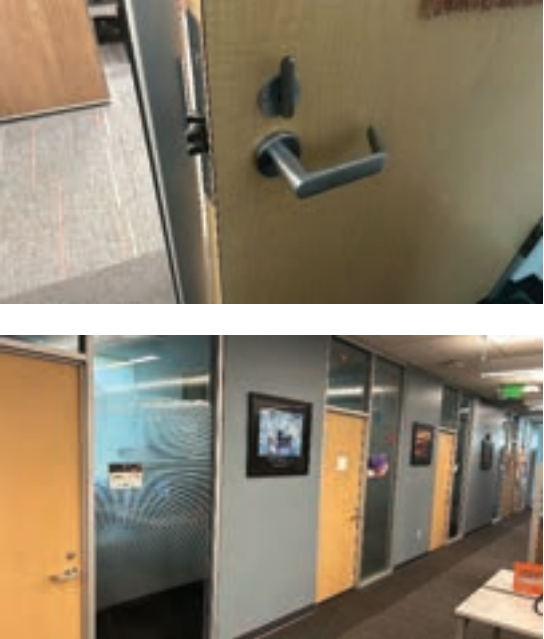
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		installed that would allow for securing access.		
35		<p>Break Rm. 112 is accessible to staff via brass key only. There is no ability to monitor which staff members enter into the room. The use of keys to access the space presents risk if an employee later is released from employment and they retain their keys. There is no formal retrieval process in operation that guarantees that staff return keys upon end of employment. Use of access control credentials would allow for immediate removal of access through systems programming.</p>	<p>Consider application of an access control card reader at this location to provide an audit trail and restricted access to the staff lounge. Develop security standards that would identify staff lounges as requiring access control measures.</p>	2
36		<p>Pass through transaction windows at the Cashier's Office have panic buttons installed on the secured side. These panic buttons are not momentarily release and require significant effort to unlock once activated. Staff shared concerns regarding this issue and shared concerns regarding accidental activation, the buttons roll-out to the Riverside Sheriff Dispatch Office. Verkada video surveillance cameras are installed in the space, there is no interface with the panic buttons for camera call-up and immediate situational awareness upon panic button activation.</p>	<p>Review the existing panic buttons that are installed and replace with momentary release buttons. Review the entire operational intent of security electronics, consider integration of video surveillance, access control, and intrusion detection to provide a unified system. Investment in security electronics should provide operational support to campus police and campus safety.</p>	3
37		<p>Cashier's Office rear entry door access is provided via remote release from an Aiphone video master station. The visibility on the camera lens at the master station does not provide a clear facial recognition of any person requesting entry. The video door station requires review and repair. Verkada video surveillance cameras are installed, but no staff members</p>	<p>Perform a maintenance review of the exterior camera to ensure that a clear field of view is provided on the internal video master station. Provide communication to the department staff regarding who can view the video surveillance cameras, and how long video is retained. Develop policy and protocol regarding video usage and retention. Security standards</p>	2

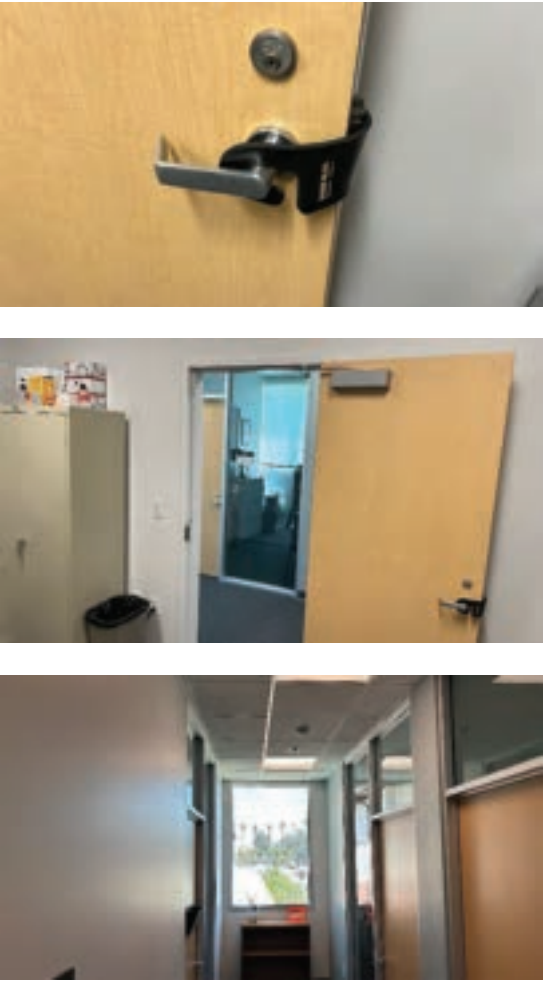

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>have any idea who monitors activity or what usage rights that persons with viewing capability may have. This is concerning from a privacy perspective that there is a lack of policy available regarding video retention and use.</p>	<p>should clearly define where video surveillance cameras will and will not be installed.</p>	
38		<p>There is no video streamed on the interior of the Cashier's Office that would provide visibility of activity on the exterior side prior to allowing entry via the Aiphone remote release function.</p> <p>Access into the Cashier's Office Rm. 111 at the main entry is through an access-controlled opening with a card reader. The space is an independent zone on the intrusion detection system which is armed and disarmed using the Software House keypad and card reader combination wall mount unit.</p>	<p>Install a video monitor above the exterior opening on the secure side to provide visibility of persons requesting entry.</p>	1

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
39		<p>The ATM machine is located directly underneath an intrusion motion sensor and a video surveillance camera. The video surveillance camera is understood to be non-operational and any theft or assault that may occur at the ATM or vending machine could not be viewed forensically if the camera system is non-operational. Non-operational cameras present liability impact issues that the district may consider as mitigating reasons for performing maintenance activity on cameras to reinstate them as operational. The intrusion arming station has been covered by an unauthorized person to attempt to silence the beeping noise annunciating from it. Self-imposed tampering with security equipment rather than communicating to the appropriate resources of a problem, demonstrates a lack of investment and enthusiasm in a security culture by some campus users.</p>	<p>Conduct a review of all video surveillance cameras and perform corrective action or replaced with new, any cameras that are non-operational. Implement policy and protocol that provides consequence and discipline for tampering with security electronic devices. Tampering with devices could inadvertently place building occupants in harm's way.</p>	3
40		<p>Data Rm. 131 is accessible by controlled entry using a security credential. The Software House access control and DMP intrusion detection head-end equipment is located within this space. The Software House iStar control boards are rack mounted, these are end-of-life and no longer available from the manufacturer as Software House ceased to</p>	<p>Consider a complete overhaul of the existing access control system to provide future expansion and integration with video surveillance and intrusion detection. Through development of security standards consider controlling all network equipment and data rooms with access control measures.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>manufacture as of 2020. The system is operational but cannot be expanded with current headend form factor. The system is not monitored by any system administrators to monitor door alarms etc., to activate response protocols (these do not exist).</p>		

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
41		<p>Controlled entry doors with zero video surveillance coverage of activity no ability to interface access control and video surveillance currently. Interfaced systems would allow for camera call-up on alarm event programming within the access control system. Real time situational awareness and forensic viewing capability is not available.</p>	<p>Monitor all exterior covered walkways and access control points providing visibility for situational awareness and forensic viewing capability. Video surveillance cameras should be programmed to provide immediate camera call up upon activation of a door forced or door held alarm event.</p>	3
42		<p>In the event of a lockdown, the ability to hide within the office spaces undetected is minimal as visibility in is unrestricted. Hardware applied to the opening is passage lock set, these locksets cannot be locked from the public or secure sides. Emergency egress is through the computer area exit door. Locking down this this space requires a brass key and mechanical locking of the main entry panic bar. Automated lockdown is not available at this building.</p>	<p>Review door hardware policy and protocol and consider installation of internal thumb turns or push buttons on all office and study spaces providing ability for doors to be secured from the interior. Consider installation of window film on all door window vision panels to restrict visibility in from the public side. Review the lockdown system and consider applying to all buildings, so the entire campus can be locked down instead of partial lockdown eliminating potential for some buildings to be automatically placed into lockdown and others not.</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
43		<p>Second floor motion detector serves no purpose as access to this floor is highly unlikely from the exterior. The glazing is inaccessible from exterior scaling of the building. Intrusion detection is typically deployed on level one of buildings and on upper floors only where direct entry into building spaces can be achieved i.e., stairwells. Public restrooms are setback from the corridor with no video surveillance monitoring of activity in the corridor or the setback area.</p>	<p>Develop security standards that provide clear direction on where security devices shall and shall not be installed. Consider installing a video surveillance camera monitoring activity on the exterior of the setback restrooms.</p>	3
44		<p>Counselors' office doors can be locked from the interior using a deadbolt throw. There are different styles of window treatments applied with no standardized process in place. Some offices have full window film applied and others none, ability to hide in a lockdown is determined by the amount of film applied to the glazing. Governance on application of film do not exist.</p>	<p>Create security standards to provide standardization and consistency across campus and the district regarding application of security measures.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
45		<p>Storage Rm. 204T is identified for shelter place use in the event of an active shooter. The door hardware is equipped with a door lock strap that covers the latch allowing for immediate closure and latching of the door when removed (the door needs to stay in a locked state to support securing of the entry upon closure without having to lock with a key). There is no means for occupants to communicate out from this space if sheltering within, other than by using personal cell phones. There is no network phone installed although data wall jacks are available to support such equipment. communication from within the space. Additionally, no emergency supplies pack was observed and there is no video surveillance installed on the exterior of the room in the corridor providing situational awareness.</p>	<p>Remove the latch retraction strap and replace with a lock block on the door frame. The door should not be propped open. Install a network phone within this space providing ability for communication in the event of a lockdown or shelter in place. Consider installation of emergency supplies for use in the event of long-term shelter in place. Install video surveillance in the corridor adjacent to the opening.</p>	4
46		<p>All office spaces have network telephones located at the work desk. The phones cannot be used for all call communications and are "old" technology NEC handsets. The deployment of telephones is restricted to office staff and telephones are not deployed within classrooms. There is a reliance upon the cell phone as the primary tool used for mass communication via push SMS messaging and the RAVE application that is an opt-in service.</p>	<p>Review the use of telephones across the campus, the pending termination of the NEC PBX service will impact further communication capability. The telephone system requires an upgrade to modern technology, and it is recommended that telephones be provided in all student learning areas i.e., classrooms.</p>	3





ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
47		<p>Access to the Administration Office space is unrestricted with the controlled entry unlocked and locked on schedule. The office space is monitored on the intrusion detection system as a separate zone with a Software House arming station/card reader wall mounted on the public side. Frosting film is applied to the individual offices and office doors can be secured from the interior using a thumb-turn deadbolt. There is no video surveillance of any activity within this space. It is understood that all staff members who function within this area have access to the data and electrical rooms at the rear of the suite which provide shelter-in-place ability. Again, there are no telephones or emergency supply kits located within the shelter-in-place designated rooms.</p>	<p>Refer to observation #45 regarding shelter in place spaces. Consider installation of video surveillance to provide monitoring of activity adjacent to the entry point. Use of remote release via video intercom would provide additional security to the occupants of the space. Install a viewing monitor within the office space providing visibility of exterior activity in real time.</p>	4
48		<p>Math and Science Building Level One offices are all controlled with access control applied to every single office. All office doors are equipped with card readers, electrified locks, door position contacts and built-in request to exit switches. Internal video surveillance cameras are believed to be non-operational. This appears typical across the campus and campus police shared frustration at limited access to video streams that could be used to proactively police the campus daily and to support incident response. The perimeter doors to the corridor are unlocked and locked on schedule.</p>	<p>Conduct a review of all video surveillance cameras and perform corrective action or replaced with new, any cameras that are non-operational.</p>	3

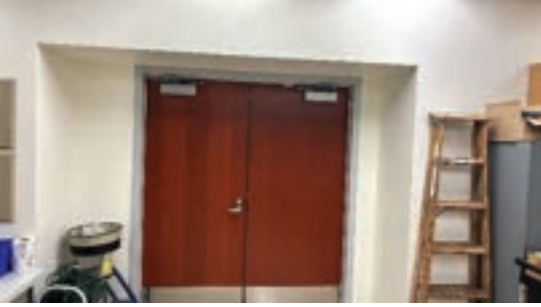
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
49	 <p>The first photograph shows a classroom door with an access control system. The second photograph shows a wall-mounted telephone. The third photograph shows a wall-mounted strobe light and a yellow emergency call station.</p>	<p>Math Building Lecture Rm. 105 has access control applied to the exterior opening and can be unlocked by presentation of a security credential twice in succession to place the opening in an unlocked state. To relock the door the security credential must be represented twice to implement locking of the hardware. This approach has risk as doors can inadvertently be left in an unlocked state if the security credential holder forgets to relock. Any doors in this state if connected to the lockdown programming will automatically be locked if a lockdown is activated. Classrooms at this building do have telephones within them, however they are old NEC wall mount devices approaching end-of-life. Glazing is above head height providing natural light with no ability to monitor activity on the exterior from within the classroom. Video surveillance cameras are installed at the end of each corridor accessible from within the classrooms (believed to be non-operational), and an emergency call station with illuminated wall mount strobe was observed (no interfaced camera call-up available upon activation of a call).</p>	<p>Review the access control system programming regarding presentation of security credentials to lock and unlock the classroom space. There is vulnerability and risk associated with this approach that is eliminated if the doors operate in a single presentation to unlock with automatic locking reoccurring on timer. Consider installation of telephones in all learning areas and review the minimum ADA mounting height requirements for devices installed on the wall. Conduct a review of all video surveillance cameras and perform corrective action or replaced with new, any cameras that are non-operational.</p>	4

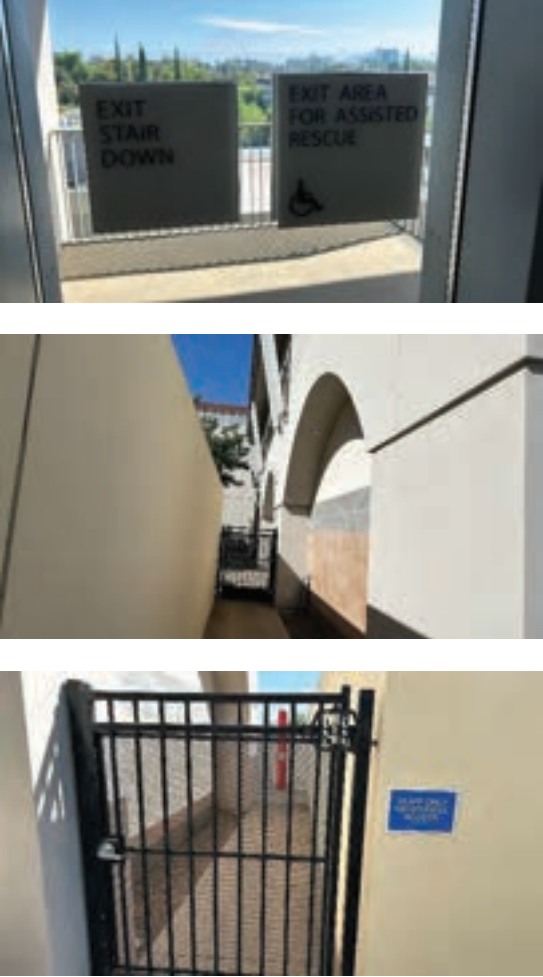

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
50		<p>Network Rm. 115 access requires a security credential be presented at the card reader. There are climate control measures installed with the HVAC temperature sensor reading 73° however the temperature was significantly higher at the time of inspection. A drip tray is installed underneath the HVAC unit, which is excellent, this is not typical at all HVAC units installed in network/data/critical infrastructure rooms. Video surveillance cameras are installed but believed to be non-operational. Camera installation does not meet typical best practices with cable loose and hanging. The battery back up in the Software House access control system enclosure was dated as installed 2017, batteries are typically replaced within the industry every two years.</p>	<p>Review the climate control measures within this space to correct the overheating risk that was observed. Consider development of a standard that ensures that all wall mounted HVAC units are equipped with a drip tray directly underneath. Recommend that a standard replacement policy regarding security electronics backup batteries be developed, replacing batteries after no more than three years from point of installation. Create design standards that provide governance and direction to architects, designers, and contractors regarding device installation best practices.</p>	3
51		<p>Emergency stairwells are accessible from each floor, once inside the stairwell there is no public reentry and exiting the building is down the stairs to the first floor. Access back onto level's 2, 3, 4, and 5 is by access control security credential only. The stairwells should not be considered general floor transition paths of travel by the</p>	<p>Install video surveillance in all stairwells as standard practice.</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>public. There is no video surveillance monitoring activity within the stairwells.</p>		
52		<p>Data Rm. 215 is a generic example of data equipment rooms located on each level. Rooms are climate controlled with HVAC units and access control headend panels are rack mounted. The iStar Software House panels are no longer manufactured. Door control panels are located above each door and cable then ran back to the iStar panel. Wireless lockdown buttons are currently being deployed across select campus buildings, activation of the button will lock all doors programmed within the system to automatically lock. No signage indicating button purpose are currently installed, and they are easily tampered with as no covers installed. Additionally, no protocol to interface with camera call-up has been considered.</p>	<p>Install protective covers over the wireless lockdown buttons to avoid potential tampering and misuse. Apply signage adjacent or above each lockdown button providing clear identification of what the buttons operational intent is. Recommend that future lockdown buttons be hardwired and mushroom form factor with protective casing. All locked down buttons should be monitored with video surveillance to provide forensic review if activated.</p>	3
53		<p>The pass-through window for distribution of chemicals and other controlled science items is secured when the space is unoccupied and monitored with a surface mount contact. The department main entry card reader is mounted to the wall within the door swing. This location is poorly designed and does not meet best practice design, locating within the door swing presents ADA access challenges and potential harm to persons presenting their security credential if a person is egressing eth door at the same time. The</p>	<p>All card readers should not be installed within the swing of the immediate door. There is potential for injury to occur to persons presenting security credentials at the card reader if an occupant of the space egresses at the same time. Remove the lockdown button and relocate within the interior of the department. Refer to recommendation #52 regarding future lockdown button considerations.</p>	1


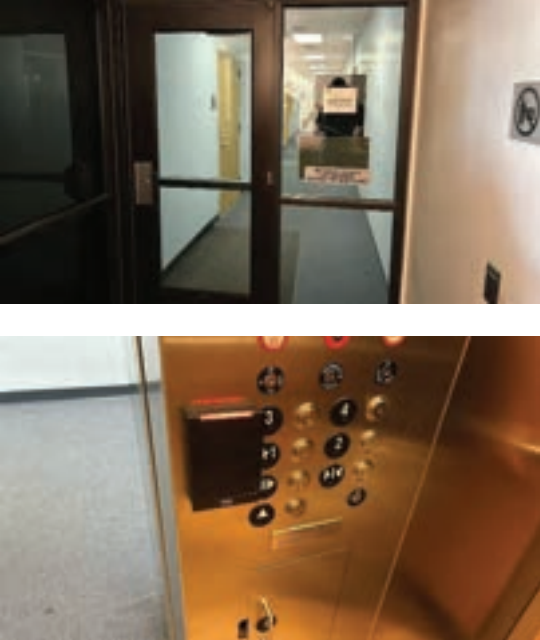

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>lockdown button has been incorrectly located on the outside of the space requiring staff to exit the department to implement a lockdown which may place them in harm's way.</p>		
54		<p>Video surveillance has not been installed to provide remote visibility, monitoring, or recording of the exterior balcony walkways, elevator access points, or exterior restrooms that are unlocked and locked on schedule and freely available for public use.</p>	<p>Recommend installation of video surveillance to provide situational awareness and forensic video review capability.</p>	2
55		<p>Placement of the emergency phone tower appears to be placed for convenience of infrastructure, rather than located in a position most appropriate and beneficial for maximized visibility of availability. The tower sits tight to the wall of the Nursing Building rather than central to</p>	<p>Review all emergency phone tower operational states. Develop an operational protocol and standard that governs emergency phone tower application. There should be standardization across the campus and district which is currently not found.</p>	4

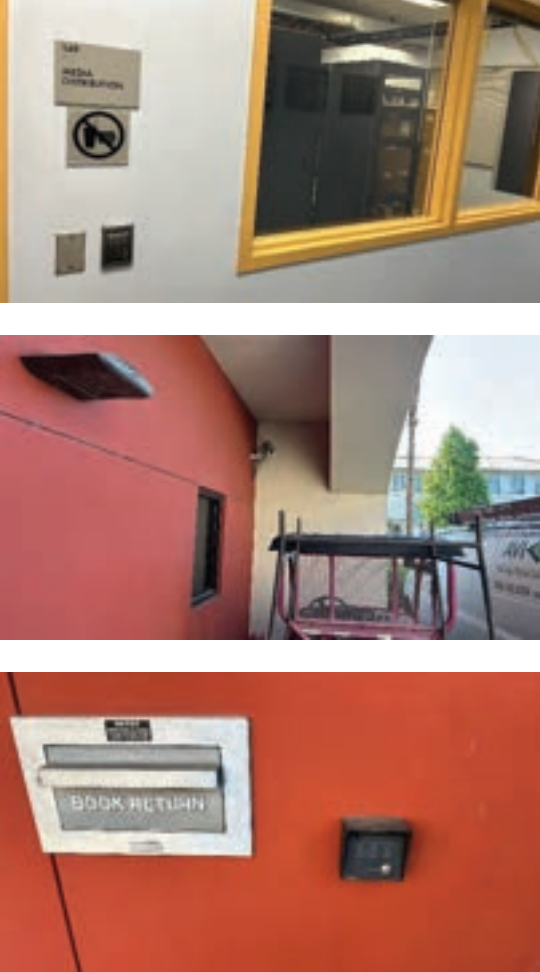

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>pedestrian walkways between the Nursing and Math's Buildings. The blue strobe on the tower is not illuminated at all times, there is inconsistency across campus on blue strobe illumination.</p>		
56		<p>The Nursing Building main entry door is controlled with an access control card reader providing after-hours access. A Software House arming station is installed to arm and disarm the intrusion system. There appears to be no dedicated ADA accessibility into this building. Video surveillance cameras are installed however they are believed to be non-operational. The area outside of the building provides seating for students which provides excellent natural visibility of activity, natural access control is also applied with paved walkways that clearly define pedestrian path of travel.</p>	<p>Review the main entry from an ADA perspective and make corrective measures if required. Conduct a review of all video surveillance cameras and perform corrective action or replaced with new, any cameras that are non-operational.</p>	3
57		<p>Glazing provides unrestricted visibility into an out of the building. There is no protective film applied to this glazing, nor is there any film applied that would reduce visibility from the exterior in. Glazing is double paned as typical for all "newer" building on campus.</p>	<p>Consider application of one-way film eliminating ability for visibility from the public side in.</p>	2
58		<p>Access into the biohazard area is accessible by two separate openings, one a controlled single-entry door via security credential and the other a double door opening via brass key. Space users confirmed that they enter by security credential only. Both openings are monitored with door position monitoring contacts. There is no</p>	<p>Review the egress requirements for this space and apply exit signs as appropriate.</p>	1

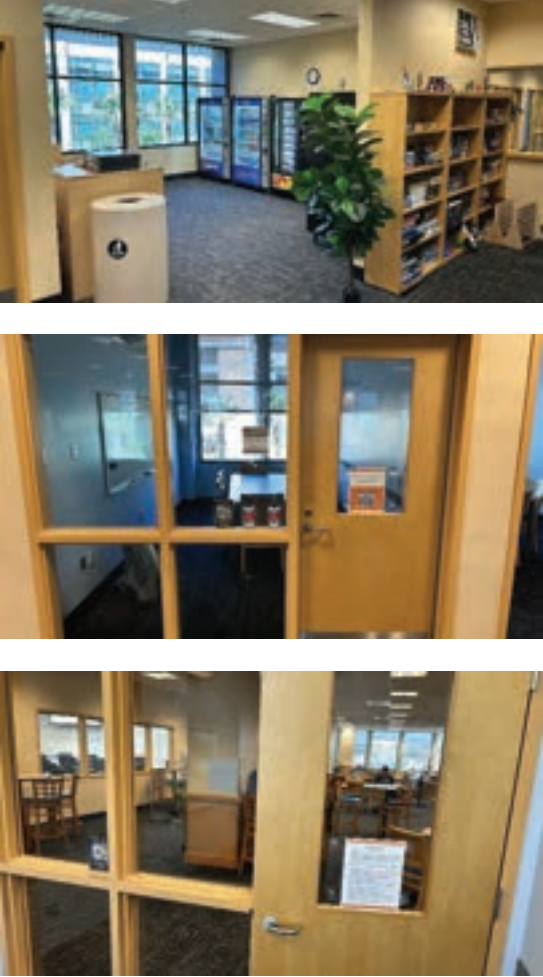

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>exit sign above either opening and no video surveillance.</p>		
59		<p>The second level stairwell landing is identified as an area of rescue with an emergency call station located within the stairwell landing. Once in the stairwell access back into the space is not permitted. There is no video surveillance camera monitoring the landing. Signage is not displayed within the stairwell providing any direction/instruction to those using it as an area of rescue.</p>	<p>Consider additional signage providing direction to those using the space as an area of rescue. Install video surveillance. Locate stairways for emergency egress as remote as possible from high-risk areas and design them to discharge into areas other than lobbies, parking zones, or loading docks.</p>	2
60		<p>The exterior landing is identified as an ADA area of rescue. There is no video surveillance camera monitoring the landing. Signage is not displayed within the stairwell providing any direction/instruction to those using it as an area of rescue, and there is no emergency telephone available for communications. The emergency phone tower is located in an area that is not identifiable from any location other than the elevated landing. A mechanical metal gate with grille has a sign positioned on the adjacent wall that states "Staff only no student access". The gate is unlocked and accessible in both directions without any</p>	<p>Consider installation of an emergency phone similar to the one illustrated in observation #59. Apply additional signage providing direction to those using the space as an area of rescue. Install video surveillance. Locate stairways for emergency egress as remote as possible from high-risk areas and design them to discharge into areas other than lobbies, parking zones, or loading docks. Consider installation of access control measures to the staff access gate to eliminate potential misuse by students.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>controls, the signage intent cannot be achieved with the physical installation in its current guise. There is no exit sign that indicates the gate is in the path of egress from the rear of the Nursing Building.</p>		
61		<p>The outdoor area adjacent to the Digital Library and the Auditorium is heavily controlled with access control applied to exterior doors including restrooms, which are locked and unlocked on schedule. There is no public address system installed that provides notification audibly if card readers are put into a locked state and building access restricted. Elevators are also controlled on a schedule; however, they are not connected to the access control system for automated locking/unlocking or monitoring. An emergency wall mounted call station calls out directly to 911 dispatch. There is no video surveillance monitoring</p>	<p>Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. The lack of communication availability to occupants within the restroom in the event of a lockdown is a liability that requires mitigating. Improve communications across campus from an information perspective providing education on the different means of receiving mass notification communications. There is misunderstanding amongst campus users, with many only aware of the RAVE mobile</p>	4



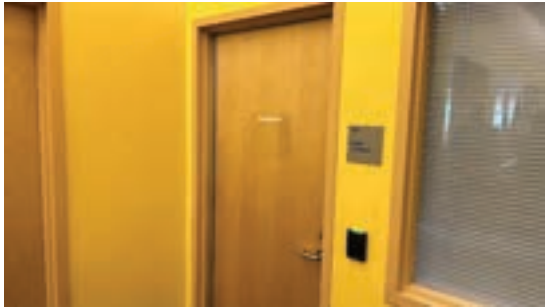

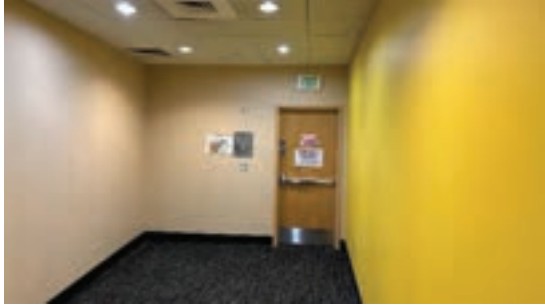
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>the area which experiences heavy foot traffic and frequent student congregation. There is good natural visibility across the area with student presence serving as eyes and ears on the ground, well-maintained landscaping supports natural surveillance, access control, and territorial reinforcement.</p>	<p>application communication and nothing else. Consider connecting the elevator controls to the access control system to allow remote locking and unlocking and schedule. Install video surveillance providing ability to monitor situational awareness activity and perform forensic review.</p>	
62		<p>Access to the Auditorium Rm. DL 121 is access controlled with a mullion mount access control card reader installed. At the time of assessment, the right leaf at the opening was not fully closed and latched. This is a vulnerability if the door is not fully secured when doors are locked on schedule. Film is applied to the glazing restricting visibility from the exterior inwards. The interior doors leading into the auditorium space were propped with a lock blok installed. Video surveillance cameras within the vestibule appear to be older technology and believed to be non-operational.</p>	<p>Perform maintenance review at the opening to ensure that positive latching occurs upon closure.</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
63		<p>The ADA access ramp is not visible from the exterior with blinds applied to the exterior glazing lowered. Egress from the main auditorium is through the side exit doors that lead out directly to the exterior exit doors. There is no video surveillance of activity within this space, or audible or visual public address in use.</p>	<p>Consider installation of video surveillance.</p>	2
64		<p>Access to the Information Support Services (ISS) area is accessible by brass key entry only, with no access control applied to the exterior opening. There is an inconsistent application of access control measures to the building. This makes no operational sense as efforts to reduce brass key distribution are hampered at buildings with access control in use at some openings but not all. There is no video surveillance within the space. The lack of security technology application at this area is surprising given that servers and other critical IT equipment resides here. Access control from the first floor upwards in the building using the elevator from within ISS requires an access control credential within the elevator cab to activate the control buttons. This has proved to be problematic (an issue of inconvenience) when access into the upper-level space from the first floor has not been possible as not all staff members have access control credentials.</p>	<p>Recommend access control measures and video surveillance be applied to this space. Critical infrastructure is housed within the department and authorized access to the space should be controlled. Consider future integration of security electronics to provide ability for security technology to serve as a force multiplier to existing campus police and campus safety personnel. Review the operational functionality of the elevator access control to determine if a better solution is available that will eliminate the problematic inconvenience issues encountered.</p>	3
65		<p>Keypads are installed within the interior space of the ISS department; however, these are non-operational and should be removed as they serve no purpose. Fully functional access control measures are not applied to the openings providing no restricted entry into or to rooms</p>	<p>Remove all non-operational keypads as they serve no purpose to the security operation. Develop security standards and apply access control measures as the standards determine. Recommend replacement of the existing audio intercom with a</p>	1


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>within the space. Video surveillance is not installed. Ability to communicate with the department occupants from the exterior if a visitor requesting entry is not available at the entry adjacent to the auditorium. A Viking intercom is installed at the loading dock opening and communication to those on the secure side of the space is operational. The video surveillance camera that is located directly outside the loading dock entry appears old and assumed to be non-operational.</p>	<p>video intercom that will provide visibility of persons requesting entry at a video master station on the secure side. Replace the non-operational exterior video surveillance camera with new.</p>	
66		<p>Access control into the main entry of the library on the second level is unlocked on schedule. There is a single video surveillance camera that is assumed non-operational, mounted in the main entry ceiling. Side rooms are equipped with passage locksets that provide no ability to lock from the interior. Visibility into the spaces is completely unrestricted with no window treatments applied. Each room is unlocked manually daily and remains in this state until relocked at the end of the day.</p>	<p>Consider replacement of passage locksets at all office spaces with internal thumb turn and lever interior locking hardware. Install window film on side room windows to restrict visibility in the event of a lockdown. Consider installation of additional video surveillance within the library area, providing visibility of general activity.</p>	4

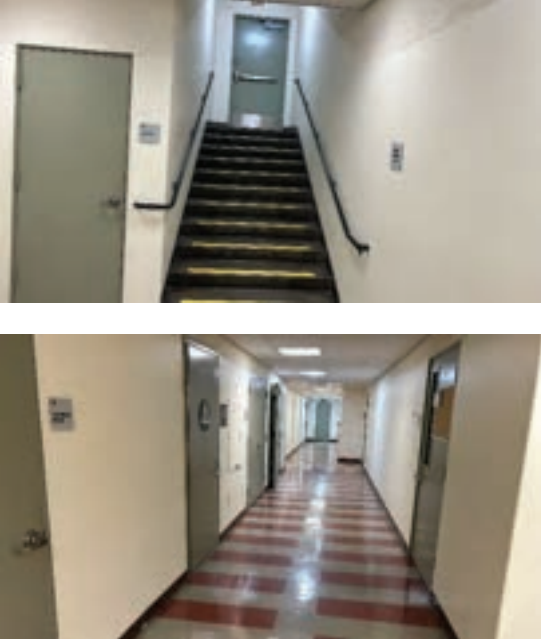


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
67		<p>The stairwell exit at the library second floor is clearly defined with exit signs above each opening and further reinforced physically at the initial stairwell exit door on both sides. There is a local door alarm that sounds if the stairwell door is opened. Signage clearly communicates visually the operational intent of the opening. Video surveillance installed in the stairwell is assumed to be non-operational. There have been concerns raised regarding the lack of re-entry available into the library space at this opening upon exiting. The opening functions as it should from a security perspective, re-entry should be through the main entry point only.</p>	<p>Install video surveillance in all stairwells typical.</p>	2

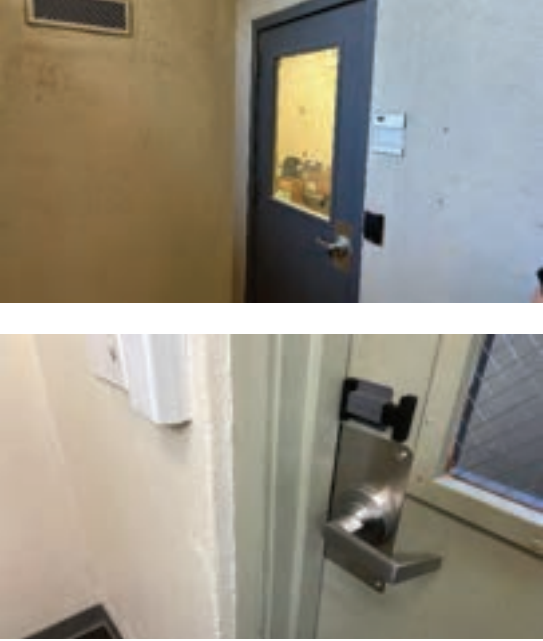
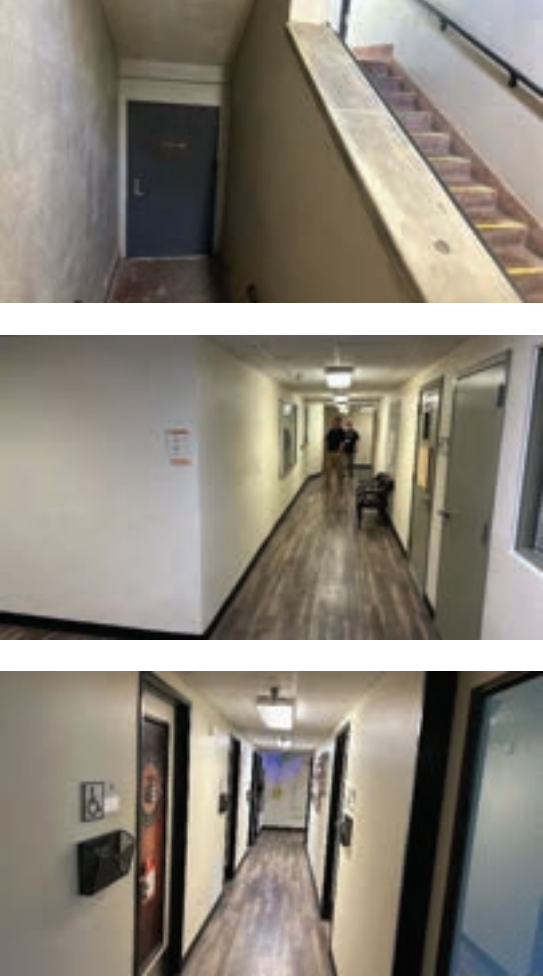
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
68		<p>A single video surveillance camera was observed on the second level of the library. A lockdown button installed behind the returns counter communicates wirelessly to the access control system. There is no signage indicating what this button does and it can easily be tampered with. Misuse or intended use places the entire campus (all buildings programmed within the access control system to lockdown). Lockdown is not available at all campus buildings.</p>	<p>Install protective covers over the wireless lockdown buttons to avoid potential tampering and misuse. Apply signage adjacent or above each lockdown button providing clear identification of what the buttons operational intent is. Recommend that future lockdown buttons be hardwired and mushroom form factor with protective casing. All locked down buttons should be monitored with video surveillance to provide forensic review if activated. Consider installation of additional video surveillance to monitor activity.</p>	3
69		<p>Camera placement monitoring activity at the elevator lobby has good intent and should be typical across campus. The access control card read installed within the elevator cab requires a security credential be presented for access to any level other than the third. From the fourth level the vantage point provides an unrestricted view of activity on level three. Ability to communicate out from within the space is restricted to personal cell phone or use of the minimally installed telephones at faculty/staff workstations.</p>	<p>Review the operational access requirements for students to the 4th floor of the digital library. Access to this space is completely unrestricted using the public stairwell, the vantage point above the library seating area presents potential risk in the event of an active shooter. If there is no operational need for students to have access to the 4th floor, recommend that current on schedule unlocked controlled entry points remain locked at all times.</p>	4




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
70	   	<p>Access to the fourth level is completely unrestricted using the main stairwell and presents significant liability and concern regarding suicide by jumping from the structure as experienced several times at the campus parking garage. The access point leading to the room that provides access to the balcony is a staff break room and controlled with a card reader but unlocked on schedule.</p>	<p>The staff lounge is unlocked on schedule as indicated in the photo with the green LED illuminated. Recommend that this opening remain locked at all times and be accessible by presentation of a security credential only. Consider controlling access to the patio with a card reader to provide additional restriction on access. Free egress from the patio shall be maintained, install video surveillance on the exterior of the patio and within the hallway leading to the staff lounge. Access control and video surveillance should be integrated to provide camera call-up if a door forced, or door held alarm is activated.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
71		<p>Access into the quad area can be achieved through several entry gateways. The gates are locked with chain and padlocks daily, with no electronic access control measures in place. Natural surveillance within the area is excellent with a seating area for students provided. The quad has a second-floor balcony providing access to rooms, also providing unrestricted visibility from a vantage point into the inner quad area. There is no video surveillance installed within the quad monitoring activity.</p>	<p>Install video surveillance.</p>	2
72		<p>Classroom doors are unlocked and opened daily by campus police and then the lock reactivated so that the doors remain in a locked state. Doors are equipped with lock blocks that support immediate closure and latching upon retraction. If a door is closed and positively latched a call has to be made to the police to come and unlock the door from the exterior as brass keys are not distributed to faculty at this building. Free egress from the interior is always maintained. Emergency blue phones are installed on both the first and second floor with the blue strobes turned on at all times, supporting ease of phone location identification. The strobe mounting heights appear close to the minimum headroom clearance required by code of 80", strobe mounting heights are not standard across campus</p>	<p>Consider providing brass keys to faculty to unlock classroom doors eliminating the need for doors to remain in an open status throughout the day. Review the mounting height of the emergency phone blue strobes to ensure that they are compliant with code driven mounting heights. Install video surveillance to provide visibility of access within the exterior walkways.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
73		<p>There is no intrusion detection system at the Quad Building with exception being the Art Gallery Rm. 140-1. Legacy motion sensors are installed sporadically within some other rooms; however, they are not operational and not terminated to the existing intrusion system. There is no video surveillance monitoring pedestrian activity on the exterior of the classrooms under the covered walkways. Additionally, stairwells are not monitored.</p>	<p>Develop security standards to provide governance and consistency of application of security measures across all campus and district buildings. Consider installation of an intrusion detection system across the entire building to provide notification and alert if unauthorized entry occurs. Install video surveillance.</p>	3
74		<p>Exterior walkway emergency telephone with blue strobe unlit demonstrates inconsistency in operational state of emergency phones and strobes across the campus.</p>	<p>Refer to recommendation #72 regarding height of the strobe mounting. Consider remounting of the strobe with a more robust wall mount arm.</p>	2
75		<p>Access into the basement under the Quad Building is unrestricted as the entry doors from the first floor are unlocked. There is no video surveillance monitoring activity into and within the basement area. Staff restrooms are accessible via brass key and are equipped with a privacy indicator. Staff are issued keys to</p>	<p>Replace existing passage lockset hardware with locking hardware. Consider controlling the exterior entry door with an access control card reader to provide audit capability, and authorized controlled entry that can be locked and unlocked on schedule. Video surveillance</p>	3


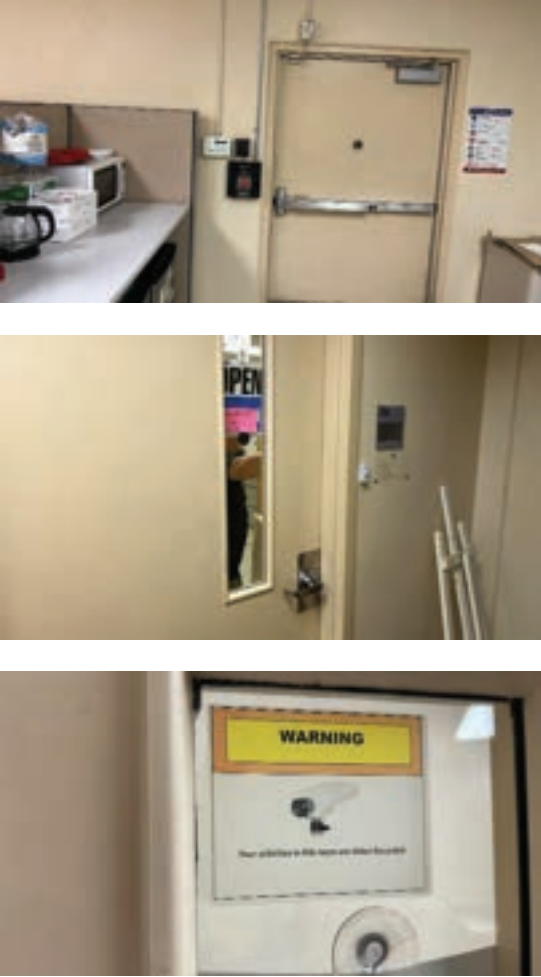
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>the restrooms but not to classrooms.</p>	<p>should be installed within the basement corridor.</p>	
76		<p>The Mail Rm. within the basement is freely accessible as the door is propped open and unlocked. There have been known vandalism issues occur within this space and there are no controls restricting access to authorized persons only. There is no video surveillance of activity in this area.</p>	<p>Recommend that all mail rooms be controlled access with access control card readers. Video surveillance should be installed within the space to monitor activity. General public should not be able to access mail rooms. Locate future mail rooms away from main entrances and areas containing critical infrastructure, utilities, distribution systems, and other important assets.</p>	3
77		<p>Rm. 100 has access control applied to it and was originally intended to serve as the Mail Rm., the controls are appropriate for a Mail Rm. A lock blok has been installed on the controlled entry door which could inadvertently hold the door open providing unauthorized access. Access control doors at non-</p>	<p>Review the policy and protocol regarding the application of lock bloks, they should not be in use at openings that are electronic entry and unoccupied spaces. All access control doors should have door closers installed on them as standard, this should be captured within security design standards. The mail room is</p>	3

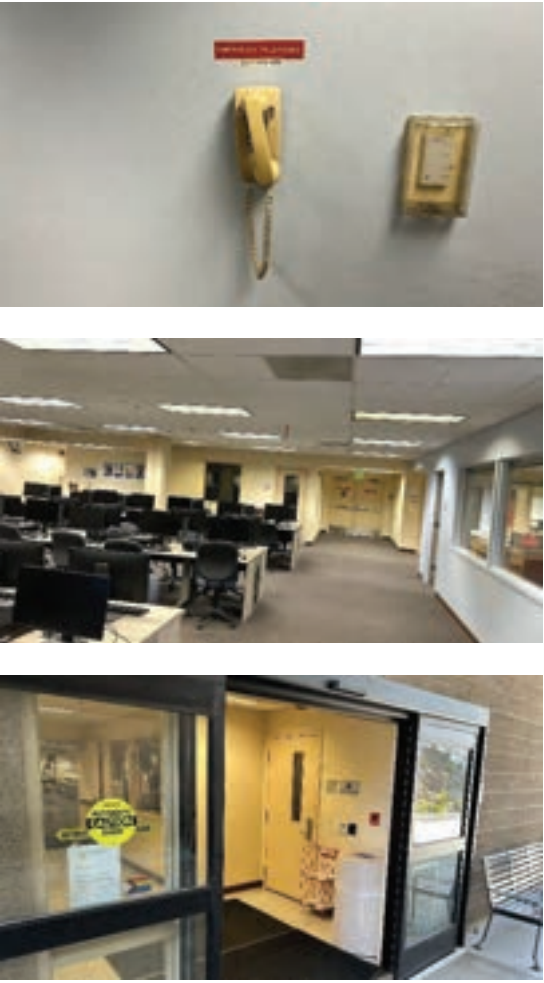
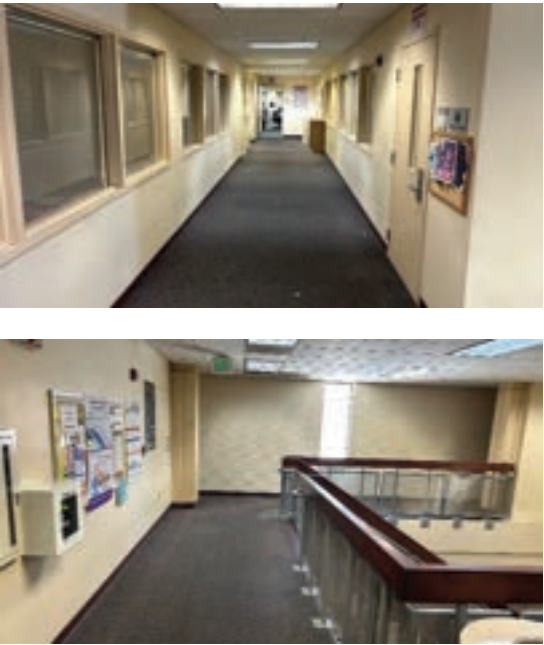
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>classrooms should not use the lock blok to avoid potential unauthorized access from occurring. Classroom 101 door was propped open with a waste bin even though it is equipped with a lock blok. Understanding of lock blok intent, and lack of operational governance regarding operational state of doors is evident.</p>	<p>located away from main entrances and areas containing critical infrastructure, utilities, distribution systems, and other important assets.</p>	
78		<p>Faculty offices located in the basement are accessible 24/7 with no video surveillance monitoring activity. The lockset is passage function and cannot be locked by key. Emergency lighting is activated 24/7.</p>	<p>Replace existing passage lockset hardware with locking hardware. Consider controlling the exterior entry door with an access control card reader to provide audit capability, and authorized controlled entry that can be locked and unlocked on schedule. Video surveillance should be installed within the basement corridor.</p>	3


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
79		<p>The emergency phone blue strobe at the Business Education building is inoperable. There is no video surveillance monitoring any activity in the vicinity. Signage above the administrative support center is clean and well displayed, however the text is small and not easily readable from a distance. Emergency lighting is installed along the underside of the exterior walkway ceiling.</p>	<p>Design text and finishes on signs for clarity and ease of reading. Perform a maintenance review of the emergency phone blue strobe to identify if it is operable or not. Develop operational standards regarding operational state and functionality of emergency phones and blue strobes. Provide consistency in application.</p>	3
80		<p>The Administrative Support Center exterior opening is equipped with a lock blok, providing ease of ingress for convenience. The door, however, at the time of assessment was found in an unlocked state requiring a person with a key to exit from the interior to secure the door before reentering potentially placing themselves in danger in a lockdown. Room numbers are stenciled onto the exterior of each door, door numbers should correlate with emergency evacuation and incident response plans for ease of identification. Stenciling font and size is inconsistent across campus.</p>	<p>Create governance that provides direction and clear communication to faculty, staff, and other campus users regarding the operational expectation of openings equipped with lock blocks. Consider replacing the door hardware at this opening with interior locking hardware to eliminate the potential risk of having to secure the door from the public side in the event of a lockdown. Design text and finishes on signs for clarity and ease of reading.</p>	4
81		<p>Classroom BE106 is equipped with door position monitoring contacts, they are legacy as this building envelope is not monitored on the intrusion detection system. Door hardware at classrooms is traditional classroom function with no ability to lock from the interior. Lock blocks are installed.</p>	<p>It is the assessment teams understanding that this building will be decommissioned. If the building is to continue to be used, recommend that the door hardware be changed to provide interior locking capability.</p>	2

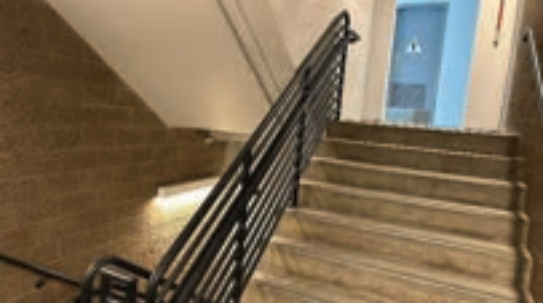
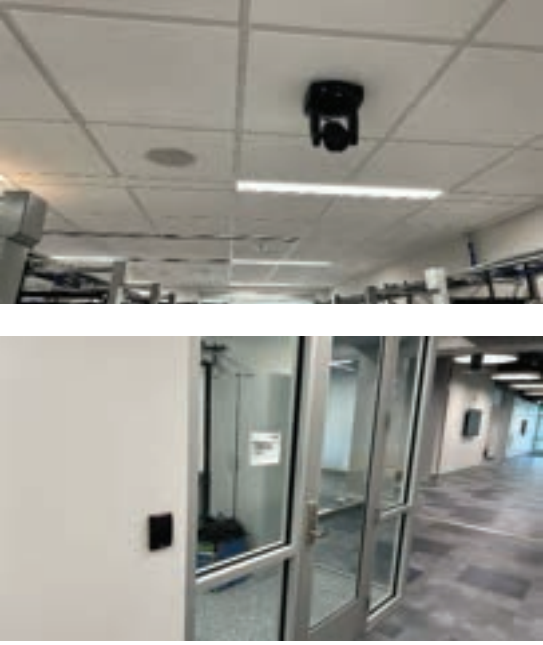
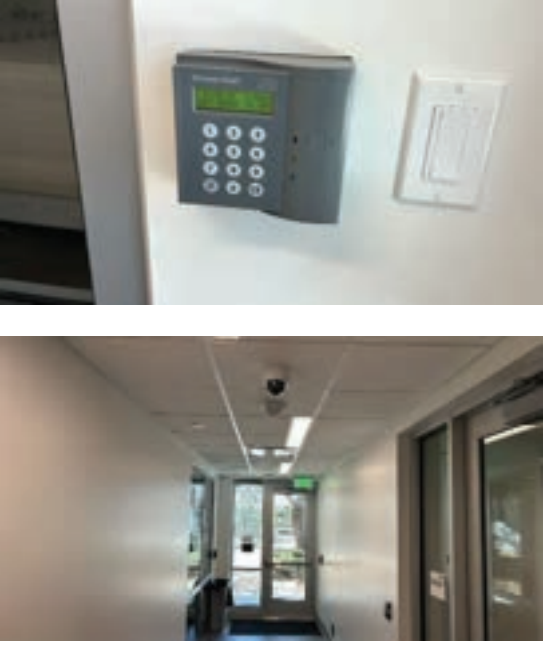
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
82		<p>The Music Building houses several different functions including offices, the Veterans Center, and classrooms. There are no intrusion detection or access control components associated with the building or video surveillance to provide visibility of activity both in real-time and forensically. Classroom 102 houses expensive forensics equipment and should be controlled via access control and monitored on an intrusion detection system. Equipment was found easily accessible in unlocked cabinets in the room. Offices within the space are accessible via brass key only, they contain telephones, but there are no telephones within the classroom spaces (this is typical across campus). There is no internal or external public address that provides immediate notification of any event on campus.</p>	<p>Install at minimum an intrusion detection system that provides ability to monitor unauthorized entry. Classroom 102 should be equipped with access control measures due to the expensive nature of the equipment located within the room. All cabinets that store expensive equipment should be locked when the classroom is not in use. Install video surveillance for general situational awareness of activity. Consider installation of telephones in all learning spaces and public address for mass communication.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
83		<p>Faculty offices have door hardware that can be locked on the interior using a push button. Window vision panels are covered by choice using a variety of material including paper, cardboard, and cloth. There is no intrusion detection system or access control system in use at the Music Hall (STVR). Video surveillance is not in use.</p>	<p>Refer to recommendation #82 regarding deployment of security electronics. The internal locking capability of the office hardware is excellent.</p>	2
84		<p>Landis Performing Arts Center is unlocked as required for events. There are no security electronics in use including intrusion detection, access control, or video surveillance. Exit from the building atrium/lobby area can occur through the identified exit openings. Emergency lighting is not installed within the auditorium. The box office collects cash on event dates only, the cash securing process should be that the cash is deposited at the cashier's office, however, this may not occur for all evening events.</p>	<p>Consider installation of security electronics to provide remote monitoring capability of the space when not in use. Review policy and protocol regarding cash collection at the box office and ensure that cash is deposited to the cashier's office at the end of each event. Review emergency lighting within the auditorium.</p>	3
85		<p>There is no access control in use at any of the Martin Luther King Jr. High Tech Center (MLK) openings. The building intrusion detection system (DMP) can be armed, using the wall mount card reader via presentation of a security credential, or manual input of a code into the keypad.</p>	<p>Develop security standards that provide a minimum baseline expectation of security electronics to be installed across all campus and district buildings. The current operational state is inconsistent with some buildings able to be monitored and locked down remotely, and others completely reliant upon</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			mechanical and human action to secure buildings in emergency situations.	
86		<p>There is no video surveillance monitoring any activity that occurs within this space. Expensive IT equipment is located here. A telephone is available at the main desk, and offices within the space are key accessed and telephones are installed within them.</p>	<p>Consider installation of video surveillance to provide situational awareness visibility and forensic reviewing capability.</p>	2
87		<p>Tech Center Network Rm. 214 is accessible via brass key, this door should be controlled with an access control card reader. There is a separate DMP arming station with card reader that allows security credential or manual code input arming/disarming of the intrusion detection system. Exterior openings are monitored by door position monitoring contacts. Signage indicating that video surveillance is in use is incorrect as the camera located within the space is inoperable. The doorbell is provided to notify occupants that assistance/entry is required/requested.</p>	<p>Develop security standards that apply security electronics to all network and data rooms. Signage should only be installed if in fact it does support the deployment of video surveillance. There is potential liability impact of signage being present without ability to provide video recorded if subpoenaed to do so. Recommend replacing the doorbell with a video intercom that provides ability for occupants on the secure side to communicate with persons requesting entry prior to providing access.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
88		<p>Level one of MLK could be accessed from level two via the elevator only, there are no stairs leading down leading down. The main point of entry into level one is via the sliding doors which provide unrestricted access via the motion sensor positioned on the door header. The intrusion detection system can be armed as on level one with a security credential at the card reader or manual input of a code. There is an emergency phone located on the interior wall, this is not consistent in form factor with other emergency phones observed across campus. There is no operable video surveillance within the building.</p>	<p>Consider applying access control to the level one main entry opening to support ability to lock and unlock on schedule. Perform a maintenance review of all video surveillance cameras across campus to verify if cameras are operational or not.</p>	3
89		<p>Level three classrooms have no access control applied to them, and doors are all opened by brass key. Windows from the corridor have blinds installed which were lowered and drawn. Classrooms cannot be locked from the inside and are traditional classroom function locksets, all classrooms have lock bloks installed. There is no governance in use that reaffirms expected operational state of doors when class is in session.</p>	<p>Recommend that all classrooms have the ability to be locked from the interior. Develop governance regarding the use of the lock bloks and communicate to campus users both faculty and students regarding the operational expectation of doors i.e., closed locked.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
90		<p>The main entry to the Building of Business and Law is controlled with an access control card reader and new Tyco manufactured multisensor video surveillance camera. This building has recently been refurbished and brand-new equipment installed.</p>	<p>General observation. The new deployment of the Tyco video surveillance cameras is inconsistent with Verkada cameras installed at the facilities building. Develop security standards that provide consistency both in application of devices and provides a standardized system and product type to be used. Inconsistency in use of disparate devices and systems is inefficient and potentially costly from a maintenance perspective.</p>	0
91		<p>Interior video surveillance camera monitoring activity within the space and activity at the single door opening.</p>	<p>General observation.</p>	0
92		<p>Cameras have been applied to monitor activity at the exterior restroom entry points and exterior walkways. This approach on a new building is excellent but emphasizes a lack of standard application of security technology across campus. Cameras have not been installed in the exterior stairwells. Public address has not been installed into the refurbished space.</p>	<p>Develop security standards to provide minimum baseline expectations of application of security electronics to all buildings. The deployment at this building appears to have been given thought regarding the application of video surveillance to monitor access points and areas of pedestrian activity. There are still gaps in the deployment in the video surveillance that should be corrected i.e., stairwell coverage.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
93		<p>Computer labs have access control applied to them and auto PTZ's that track movement within the space.</p>	<p>These measures are excellent, consider applying window fill to the glazing to obscure visibility from the public side.</p>	0
94		<p>The intrusion alarm system can be armed/disarmed by presentation of a valid security credential at the Software House arming station. Tyco video surveillance cameras are installed within the building monitoring access control entry points throughout. The intrusion detection system is not utilizing ceiling or wall mount motion sensors and is reliant 100% on door position monitoring contacts installed at each exterior opening.</p>	<p>General observation. Future development of security standards may determine that in addition to door position monitoring contacts, that internal motion sensors be applied to the intrusion detection system deployment.</p>	0

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
95		<p>Head-end security equipment is located on the first floor at Rm. 118 with controlled entry to the room. The room is climate controlled with the temperature set at 70°, a drip tray installed under the HVAC unit is excellent and should be typical across the district. The Tyco American Dynamics network video recorder, rack mounted, requires some cable management and labeling to meet installation best practices.</p>	<p>General observation. The installation of the security head end equipment is excellent with final cable management to be completed prior to the building being officially opened.</p>	0

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
96		<p>The request to exit motion detector (REX) is mounted on a pole from the ceiling, the REX can be avoided by walking directly adjacent to the wall behind it to exit the building. Bypassing the REX will cause nuisance door forced alarms on the access control system. The Tyco multisensor video surveillance camera is pole mounted approximately 8' above finished ground and is easily within reach to be damaged/tampered with.</p>	<p>The deployment of the new security equipment has some challenges from an operational state. Consider adjustment of the REX sensor to the door frame header ensuring that all persons exiting will trigger a door contact shunt within the access control system to eliminate false alarm events. Minimum camera installation heights should be 10' AFF. Development of security standards would help provide direction and minimum installation expectation for future systems upgrade and roll out. Final systems testing reports should identify if the REX sensor has been bypassed on exit and door forced alarm events received.</p>	2
97		<p>An Emergency Responder Radio Communication System (ERRCS) is installed within this building. An ERRCS is an amplification system that receives public safety radio signals from an off-air donor antenna and re-transmits them through in-building service antennas. The building has been refurbished and the core block material remained.</p>	<p>General observation.</p>	0
98		<p>The Deans Suite will operate in an unlocked state during typical business hours. There is no panic button located at the suite main reception desk and it is assumed that there is one within the Dean's Office. There is no ability on the interior of the suite to monitor general area activity using video surveillance, this is a high-profile occupancy space.</p>	<p>Install a panic button at the main reception desk to provide potential early notification of request for assistance. Recommend that a video monitor be installed at the reception desk to provide visibility of activity in the immediate area of approach to the suite. Although the intent is for the suite to be accessible to all during normal hours of operation, consider installation of a video surveillance intercom with remote release unlocking of the door to provide ability to screen persons prior to gaining entry.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
99		<p>The Facilities Department is accessible through door 101 which remains unlocked throughout the day. The door can be secured from the interior using a thumb turn on the lockset. The building is monitored using door position monitoring contacts on the intrusion system and can be armed/disarmed using a manually input code. There is no internal video surveillance installed and minimal exterior video surveillance monitoring general activity. Verkada video surveillance cameras are in use, however, no one within the facilities department has ability to view the camera stream. Video surveillance across the entire campus is underutilized to support operations, safety, and security.</p>	<p>Develop security standards to provide a minimum baseline expectation of application of security electronics across all buildings. This building has no ability to be locked down remotely and access into the space is completely unrestricted. Consider controlling entry into the building and installing a video intercom to provide ability to screen persons prior to granting access.</p>	3
100		<p>The chain-link swing gate at the facilities department is closed each evening. The height is 6', easily scalable, providing no deterrent to persons with intent to cause harm from easily accessing the yard without permission. District vehicles are parked adjacent to the hillside which can easily be accessed from the street above.</p>	<p>Review existing fence, gate heights, and consider installation of fence toppers to provide additional deterrent to potential unauthorized scaling. Install a fence at the top of the embankment adjacent to where the district vehicles are parked to mitigate the current ease of access. Install additional video surveillance providing complete</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
			<p>visibility of all activity in the facilities yard which has experienced theft.</p>	
101	  	<p>The warehouse is monitored with an intrusion detection system, and access is by use of brass key. As with the facilities gate, the fence line is 6' in height and easily scalable. A Verkada video surveillance camera provides video monitoring of activity.</p>	<p>Apply access control to the facilities building and warehouse to provide ability to perform audits to identify who accessed the spaces and when. All security electronics should be integrated to provide ability to support real time awareness and forensic investigation.</p>	3
102		<p>The warehouse receiving area has no video surveillance monitoring. The landscaping adjacent to the warehouse is well-maintained, providing minimal area for people to loiter and potentially conceal themselves without identification. Speed restriction measures on the access road is</p>	<p>Refer to recommendation 101 regarding application of security electronics. Perform a review of all existing signage deployed across campus and consider installation of additional signage that provides clear speed limit expectations to vehicle users.</p>	3


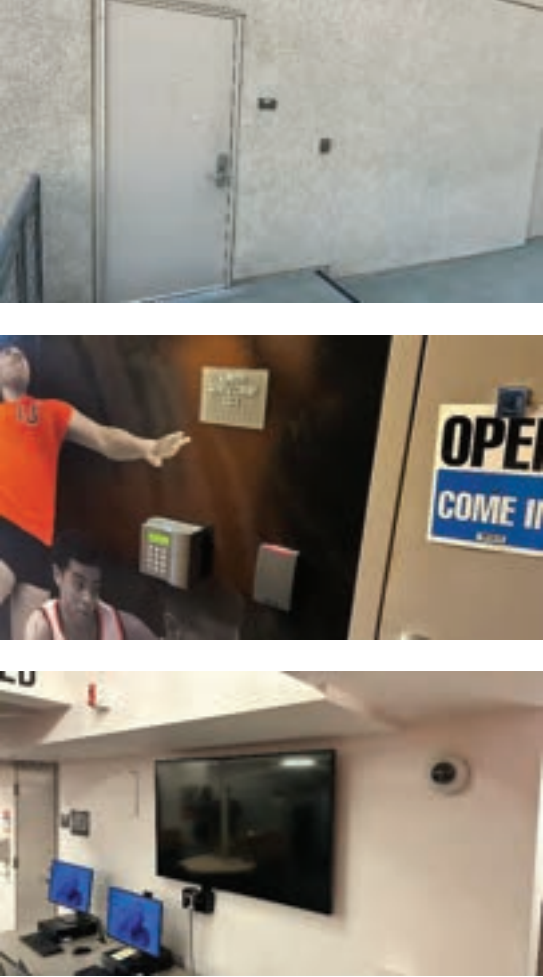
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>limited to speed bumps with no speed limit signage displayed to provide governance.</p>		
103		<p>The Pilates Studio (PLTS) is set back from the road and access is via brass key opening of doors. The hardware consists of pull plate trim only. Downwards cut off wall mount LED lights are located above or close by exterior openings, which is excellent. General signage and wayfinding across the campus is extremely poor and it is difficult for visitors to easily identify where they are located on campus. There is no video surveillance monitoring any activity in the area adjacent to the PLTS and the Gymnasium (HG). In addition, there is no exterior public address that will provide audible announcement and communication of information in an emergency. Signage at the PLTS doors is minimal in size and not stenciled on the physical doors themselves. Inconsistency in door numbering demonstrates a lack of standardization in process/application of safety and security measures across campus.</p>	<p>Perform a review of signage and wayfinding in use across campus and provide standardization of font and text. Design text and finishes on signs for clarity and ease of reading. Exterior lighting deployed above each of the openings in this area is excellent. Install video surveillance.</p>	3
104		<p>Access to the gymnasium (HG) was freely available with no restrictions on access to the gym or changing rooms. All doors were propped open with intent assumed to provide airflow into the gymnasium space and access into both the women's and men's restrooms. There is no emergency phone located within</p>	<p>Review the operational state of the gymnasium, do all doors need to remain open and unlocked at all times providing complete free ingress? Recommend that an emergency telephone be located within the gymnasium space and an emergency phone tower or wall mounted emergency phone be</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>the vicinity of the PLTS and HG exterior area. Access control, intrusion detection, and video surveillance technology is not deployed in any state at this location. Further inspection identified that there does not appear to be a telephone located within the gymnasium for use during an emergency. Public address as typical is not installed.</p>	<p>installed on the exterior. Develop security standards to determine minimum baseline expectation of security electronics application to buildings.</p>	
105		<p>The main covered parking structure is 5 stories and accessible from both lower and upper campus with no vehicle barriers to provide speed constraints upon vehicle entry/exit. Roller gates are installed at the lower campus point of entry but remain open typical. At the lower entry video surveillance does not monitor activity, previous video surveillance cameras have been removed and not replaced, cable remains. Emergency blue phone strobes appear to be installed below ADA 80" minimum height requirement for protrusion. Emergency call boxes are located consistently on each level, they appear aged and in need of</p>	<p>Perform a review of the mounting heights of the ADA blue strobes. Consider use of all-in-one call station and blue strobe units in the future that do not protrude more than 4 inches from the wall. Consider installation of video surveillance at the entry and exit points to provide monitoring capability of vehicle activity. Review the use of the level 1 gates and determine if there is operational benefit to closing on schedule to restrict access into the parking lot. Control entry measures would be required on the upper level 5 entry.</p>	3




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>replacement with single combined speaker/strobe units. There is no camera monitoring call stations or general activity within the parking lot structure on the lower levels.</p>		
106		<p>Emergency phones are inconsistent in their performance with some strobes powdered at all times and others not. Camera's cable is still protruding from the conduit at the location from where the camera was removed. Speed bumps are installed to help reduce vehicle speed, and on the tarmac, there is speed limit signage painted. This is hard to read and states a 5 MPH speed limit, there is no physical signage on the walls further supporting the speed restrictions. During the assessment vehicles were observed bypassing the speed bumps and driving at speeds significantly higher than 5 MPH.</p>	<p>Reference recommendation #105 regarding emergency phones, all emergency phones across campus should operate in a standardized functional state. Legacy camera cable should be demolished. Reinforce speed control signage by repainting the tarmac signage and installing physical speed limit signs.</p>	3
107		<p>On Level 5 at the parking lot in Equipment Rm. 510 there is legacy video surveillance head end equipment. There is no login known by the Safety Team providing access to view video. The assumption of the team is that the video surveillance cameras are non-operational. There are several cameras post mounted on the upper deck of the parking structure. Elevators at the parking lot are accessible 24/7 as there are no timing controls to support locking them down on schedule.</p>	<p>Consider controlling the elevator locking schedule by using the access control system to provide remote management capability. Review the parking lot video surveillance system and determine if there is a current logging that will provide ability to view cameras. Recommend that the entire security electronics system be reviewed, and future state be a fully integrated unified platform.</p>	2

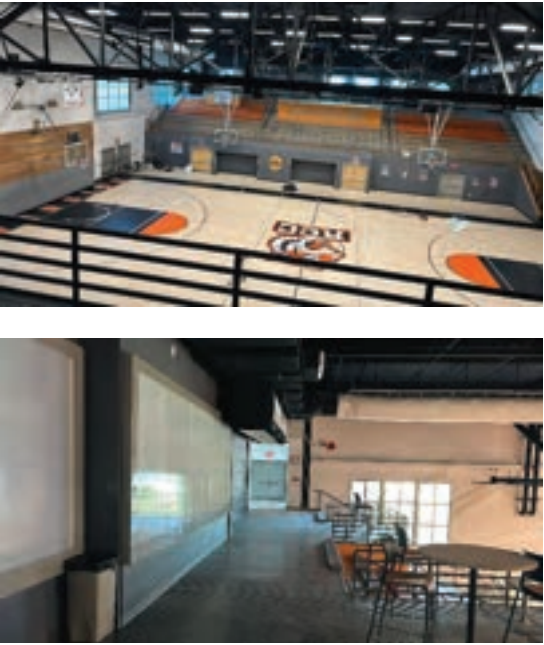

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
108		<p>Access to the Sports Complex can be achieved on foot through a pedestrian tunnel that has lighting within it. The press boxes and clubhouses at the field area are monitored on the intrusion detection system. There is no access control or video surveillance installed in this area. Emergency call boxes appear aged and requires a painting refresh, inconsistency in performance of the strobes is evident as the blue strobes are not eliminated for ease of identification as they are with others across campus.</p>	<p>Apply intrusion detection to the press rooms and clubhouses to provide ability to monitor and receive notification if unauthorized entry is made. Replace the existing emergency call boxes with new. Identify/create a district standard and apply.</p>	4

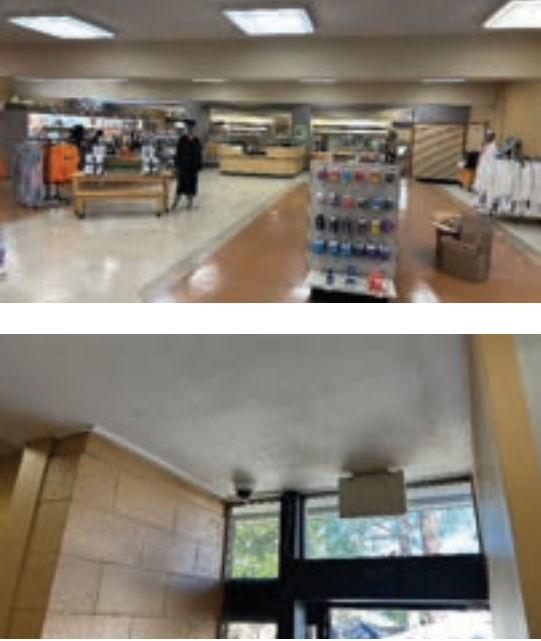


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
109		<p>Access to the Ceramics Building (CS) is through two mechanical openings only. The openings are both equipped with lock blocks, and the doors can only be locked from the exterior side. There is no intrusion system within the building and no exterior video surveillance. All windows are equipped with ceiling to floor curtains that allow for restriction of visibility from the exterior side in when drawn.</p>	<p>Apply security electronics to allow monitoring of the space from an intrusion and access perspective and apply exterior video surveillance for visual monitoring.</p>	3
110		<p>Access into the Art Building (AR) is unrestricted when doors are unlocked. There is no intrusion detection system, video surveillance, or access control applied to the building. Building identification signage is inconsistent across the campus; different signage sizing, fonts and material type are in use both on buildings and door openings. There are window treatments applied to the exterior glazing which were observed as closed restricting visibility in from the exterior. Access onto the upper deck area is restricted.</p>	<p>Apply security electronics to allow monitoring of the space from an intrusion and access perspective and apply exterior video surveillance for visual monitoring. Install a camera on the upper deck to monitor activity. Standardize on signage font and size across campus to provide uniformity in approach and promote standardization and culture.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
111		<p>Entry into the Gymnasium (WG) can be achieved at several points of entry. There are access control measures applied with electrified hardware. There is no pattern of video surveillance being installed at access-controlled entries to monitor ingress/egress activity. Some controlled entry points are unlocked/locked on schedule for convenience of staff, faculty, and student access. The building has an intrusion detection system that can be armed/disarmed using a security credential or manual code input. A video surveillance camera was observed within the learning center space, this is an anomaly across campus where interior cameras are typically not monitoring internal working/learning space.</p>	<p>The security electronics in use at the gymnasium are excellent, recommend that integration of video surveillance with the access control and intrusion systems occurs. Future security standards should provide direction regarding application of video surveillance to monitor controlled entry points providing camera call up ability.</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
112	 <p>The 'PHOTO' column contains four images: 1) A server rack with a Sony NVR unit. 2) A network switch with a camera and a Sony NVR unit. 3) An open server rack showing internal components and a Sony NVR unit. 4) Two intrusion detection panels mounted on a wall.</p>	<p>MDF 109 at WG is access controlled entry. The Sony network video recorder (NVR) installed within the equipment rack. Sony cameras are no longer manufactured or supported by Sony, this is another example of disparate video surveillance being used across campus with no unified or integrated approach to security technology in operation. Accessibility to the video stream from the network video recorder is unavailable to campus safety. The Software House headend access control equipment and the intrusion panel are also installed within the space. An Inovonics wireless receiver is mounted above the DMP intrusion enclosure. The room is climate controlled with no drip tray mounted under the HVAC unit.</p>	<p>Recommend that a review of the security electronic system administration process and ownership occur. Identify or create a definitive security systems administration role assigning responsibility of management of all the systems from a central control point. The current lack of systems ownership provides inefficiencies to the safety and security program at the college. There are several different stakeholders who require access to different components of the security system, but there is no single point of ownership currently in place.</p>	4




ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
113		<p>Wall mounted PTZ cameras are located adjacent to each controlled entry point on the north side of the building, overlooking the parking area. It is not possible to determine if the cameras are in a "home" position or if the field of view is being controlled remotely. Access control is applied to openings within the space, with access to the teaching area and gymnasium is typically unlocked on schedule.</p>	<p>Develop security standards that provide direction and guidance on how PTZ cameras should operate. Recommend where PTZ cameras are installed that supplementary fixed field of view cameras also be installed monitoring-controlled entry points.</p>	3
114		<p>The gymnasium level two elevator landing adjacent to offices which are all equipped with access control card readers is monitored by a video surveillance camera. A "Help Phone" installed on the wall does not provide any identification or instruction relating to who will respond to the call when activated. Camera call-up with the video surveillance camera is not available.</p>	<p>Apply signage above the help phone that provides information on where calls will be answered when placed. Consider future systems integration allowing camera call-up capability when door forced, or door held alarm events are received within the access control and intrusion detection systems.</p>	2



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
115		<p>Inside the gymnasium there are no cameras monitoring activity across the floor area or within the bleachers.</p>	<p>Consider installation of video surveillance to monitor general activity, this is typical across education institution gymnasiums.</p>	3
116		<p>Emergency phone call tower located at the rear of the gymnasium is another example of inconsistent tower coloring, inconsistency in manufacturer unit being used, and the blue strobe is illuminated. The data access enclosure is not secured with a padlock and easily accessible for tampering with cable.</p>	<p>Reference previous recommendations provided regarding standardization of emergency phone towers. Apply a padlock to the cable access enclosure.</p>	4

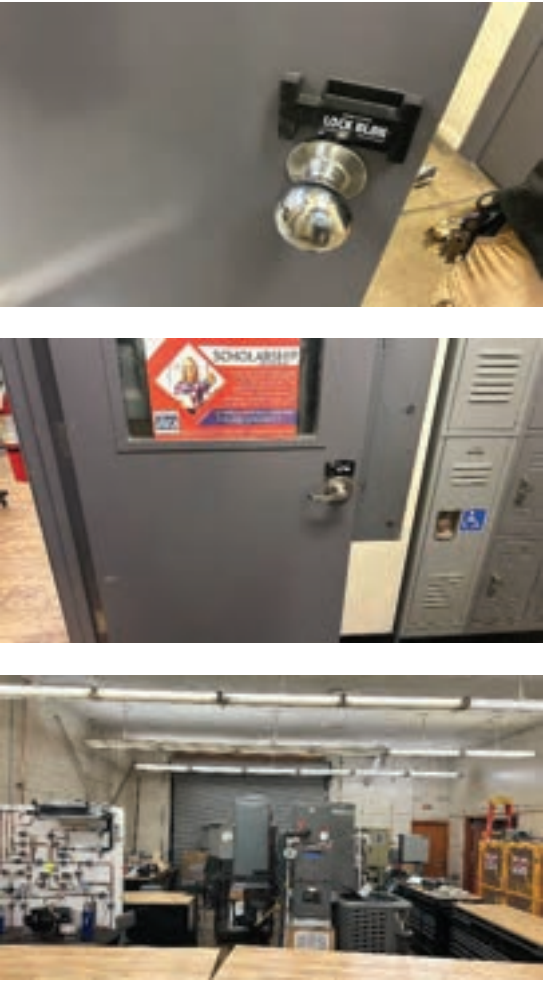

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
117		<p>The bookstore (BKST) is a campus owned space that is managed by a vendor. The space intrusion components are not part of the campus intrusion detection system, neither is the video surveillance installed within this area. Vendors are required to register as part of the RAVE mass notification application so that they receive alerts if the campus goes into lockdown etc. There is no interior public address system or campus telephone available.</p>	<p>Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. A campus wide public address system should be considered.</p>	0
118		<p>The Student Center Building is unlocked/locked on schedule manually by brass key by the campus police department. Interior offices are key controlled with lock blocks installed, there is no ability to lock the doors from the interior of each office space. This building has no access control, intrusion detection, or video surveillance applied to it. Unrestricted ingress is available from the moment that the exterior doors are unlocked.</p>	<p>Consider application of access control to support remote unlocking/locking on schedule. Install intrusion detection to monitor the building outside of normal hours of operation. Install video surveillance integrated with access control and intrusion detection systems for real-time situational awareness and forensic viewing capability. Upgrade existing door hardware to provide interior locking capability at offices and learning spaces.</p>	4
119		<p>Video surveillance cameras within the Cafeteria terminate within the office of the Food Services Director. This is a standalone system not accessible by campus safety or campus police. Network cables are clearly labeled terminating into the patch panel in the wall mounted data rack that was</p>	<p>Incorporate the video surveillance cameras into a campus wide and district video surveillance system.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
	   	<p>unlocked. Camera performance appears adequate for their application and can be viewed locally on the monitor with the Food Services Director's office.</p>		
120		<p>Healthcare services mental health assessment rooms have ability for the door to be locked on the interior with a thumb turn. Help buttons requiring two button activation are located under the work desk. These are tested frequently by the campus safety team. The panic buttons are wireless and also located throughout the building at</p>	<p>Consider replacement of the existing two button activation panic buttons with single momentary activation buttons. Recommend that all panic buttons be hard wired rather than wireless to provide ability to be supervised on the security electronics systems.</p>	4



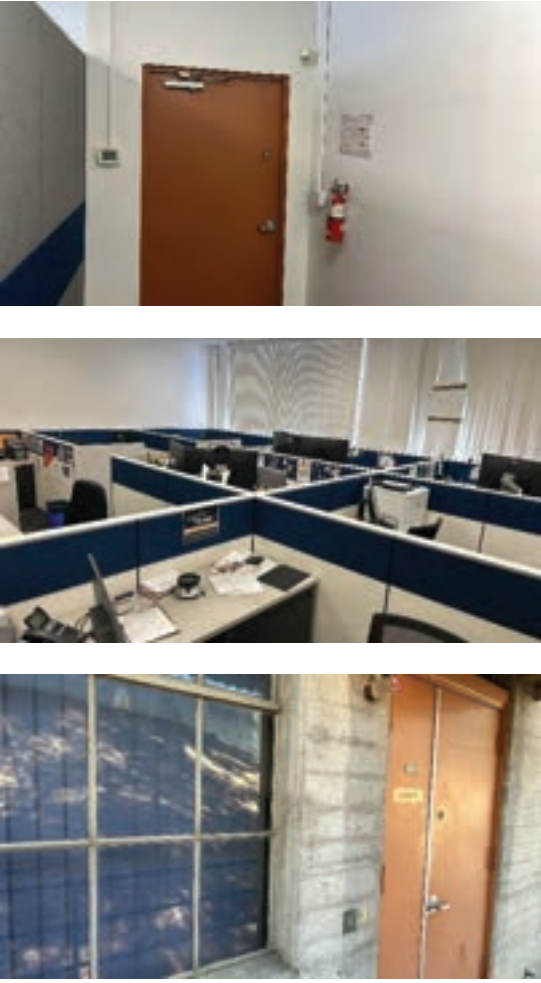
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>sporadic workstations. Treatment room door vision panels are obscured for privacy. There are no drugs/narcotics stored within the space, but Narcan is available and stored within a locked cabinet.</p>		
121		<p>The network operation center (NOC) is located within the Information Security Building. This building is not controlled with any access control measures or video surveillance on the exterior of the space which is highly unusual for such space use. The exterior entry door is not equipped with a door closer to support positive latching upon closure. An intrusion detection system (DMP) is installed, video surveillance cameras on the interior of the NOC include Axis and Sony manufactured devices. There is no consistency in video camera manufacture edge device in place at the campus. It was shared during the walk that the</p>	<p>Apply access control measures and integrated video surveillance to the NOC. Access into this space should be controlled on a permissions basis using the access control system. A door closer should be installed on the exterior door to ensure that positive latching occurs upon closing. The PBX should be replaced with new and support future expansion of standard and emergency communications across the campus.</p>	3



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
	   	<p>NEC private branch exchange (PBX) will soon become obsolete; and telephone lines are also being discontinued by AT&T as they go out of service. A portable generator is located outside of the building to provide power in the event of a power outage.</p>		
122		<p>The Automotive Technology Building (AT) houses some of the most valuable equipment on campus. The space is completely open to public access during the hours of operation and there is no access control, video surveillance, or intrusion detection systems installed. Access into the yard can easily be achieved from above, and the</p>	<p>Consider installation of all security electronics systems to provide controlled access into the space after normal hours of business, unlock/lock of the space on schedule, and provide video surveillance monitoring of activity. Minimum 8' high fencing and gates should be installed around the entire perimeter of the AT building.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>perimeter wall can simply be scaled as it is no higher than 7'. Gates are closed and locked with a padlock; however, they are chain-link and could easily be driven through from the exterior or interior sides using a vehicle. There have been documented thefts of equipment from the space over the years; AT spaces typically would be monitored for unauthorized activity.</p>		
123		<p>Lock bloks are deployed at Technology A (TECH A) classrooms however, some classrooms have recently had doors repainted and the lock bloks need to be reapplied. There is high value equipment within this building, including welding and HVAC and it is recommended that security technology be applied, at</p>	<p>Reapply the lock bloks and install an intrusion detection system with the roller doors monitored with surface mount door monitoring contacts.</p>	4



ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>minimum an intrusion detection system. Roller doors leading directly to the exterior are not monitored and provide ease of access to remove equipment if breached.</p>		
124		<p>Benches and seating areas provide areas of excellent natural surveillance and eyes on activity. Power is provided at the covered workstations supporting use of the tables for students to use. The seating area is elevated providing excellent visibility of the parking lot on the lower campus. The pole mounted emergency phone does not have any signage clearly indicating that the emergency phone is located here, and the blue strobe is not illuminated. The call station is manufactured by Trigon and is no longer available.</p>	<p>Perform a review of all emergency phone towers and call stations. Standardize on one product manufacturer and replace end of life and non-operational emergency phones with new. Install signage that clearly indicates the location of the emergency phone tower.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
125		<p>As with Tech A, the Tech B building has zero security electronics installed and monitoring or notification of activity cannot be monitored in real-time or forensically. There is a vantage point that provides oversight of activity of the yard below. Chain-link fencing surrounds the yard area and is secured in the evening. Scaling of the fence and gates can easily be achieved as height is approx. 6'.</p>	<p>Consider installation of all security electronics systems to provide controlled access into the space after normal hours of business, unlock/lock of the space on schedule, and provide video surveillance monitoring of activity. Recommend fence line height be a minimum 8' in height.</p>	3
126		<p>The district printing and graphics area located within Tech B houses expensive equipment. At a minimum intrusion detection should be applied to this space, and the space designated as a single zone. Access into this space is via brass key only issued to restricted authorized personnel.</p>	<p>Install both intrusion detection and access control systems to this space. Ability to be alerted and notified if unauthorized entry is achieved should be available. Video surveillance should monitor activity on the exterior of the space.</p>	3


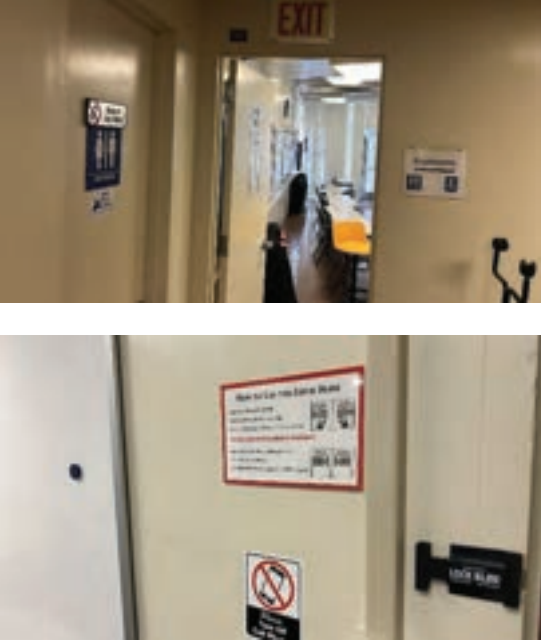

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
127		<p>A sign indicating that the space within Tech B is a designated watch area is an anomaly across campus. This sign was not observed in any other location.</p>	<p>General observation.</p>	0
128		<p>Access at the Tech B district only space is accessed through a brass key-controlled opening which was unlocked at the time of assessment. There is no access control applied to the space and existing intrusion surface mount door position monitoring contact and wall mount motion sensor do not communicate to any operable system. It is unusual for the district to have a space on a campus that is not controlled with restricted entry, if no requirement for access by students or others. Visibility into the space is restricted from the exterior as window treatments are drawn, there is no communication or notification capability i.e., intercom or doorbell that would support closing and locking of exterior doors to this space at all times.</p>	<p>Recommend that security electronics be applied to the district access only space. Install a video intercom providing ability to communicate with persons on the public side requesting entry if they are not authorized via security credential.</p>	3


ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
129		<p>The Gateway School utilizes the portable classrooms L4 through L9 with a combination of offices and classrooms. Classroom doors cannot be secured from the interior side however, they are equipped with lock blocks, offices do not have lock blocks. The school staff are part of the RAVE mass notification application opt-in program. There is a legacy DSC intrusion arming system installed however, this is non-operational, and the portables are not monitored on the district intrusion system. There are no access control and video surveillance measures in place.</p>	<p>General observation. The Gateway School determine their own operational policy and protocol.</p>	0
130		<p>Campus Police occupy the portable spaces L1, L2 and L3. They operate with their own independent keyway with limited district access. No access control, intrusion detection, or video surveillance is applied to these portables. Doors are equipped with latch guards that prevent potential forced entry by tampering with the latch. The</p>	<p>Recommend that the campus police offices be accessible by access control, and intrusion detection be installed with exterior video surveillance. Campus police should be provided access to monitor all security electronic systems.</p>	0

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>campus police are not on campus 24/7 so times of inoccupation of the space is frequent. Direction to the Campus Police Offices is not provided throughout the campus, minimal wayfinding signs and maps make it difficult to know where to locate campus police. The portables windows are hardened with metal grates placed over them, visibility in is not possible from the public side.</p>		
131		<p>Restrooms adjacent to portables L12, L13, and L14 are unlocked by campus police daily and remain unlocked throughout the day. The restrooms are freely available to campus users and the public. There is no video surveillance deployed in the vicinity that provides both situational awareness and forensic viewing capability. An emergency telephone is located on the edge of portable L14 however this is not visible from any other area along the adjacent road and is the only emergency phone located in the immediate vicinity of the portables and tennis courts. Signage does not provide any direction to the emergency phone location.</p>	<p>Install video surveillance to provide monitoring of activity on the exterior of the restrooms. Consider relocating the emergency phone into a more prominent position that better serves the area adjacent to all of the portables. Provide signage that clearly indicates the location of the emergency phone.</p>	2
132		<p>The Riverside Aquatics Complex (RAC) has no security technology applied to it. Swimming pools are typically high liability impact areas that education institutions seek to have visibility of activity and restrict unauthorized access into. There is a known incident of an unauthorized user using the facility and causing themselves harm. The perimeter fencing is decorative and has a flat top rail that supports easy scaling, the exterior gates can also be easily scaled. Emergency phones appear to protrude more than 8"</p>	<p>Install security electronics to the RAC, consider replacement of the existing fence line with new increasing the height and reducing the ease of current scaling. If needed engage with the City to ensure that there is full agreement on application of security measures. As stated, this area present significant liability to the district and should be addressed. Video surveillance should be installed on both the exterior of the RAC and within the pool deck.</p>	4

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>from the wall and may require review against ADA "cane wall" mounting code. Visitor parking spaces are identified across campus by the white bays and yellow bays for faculty/staff, this system was observed at the RAC. The RAC is a shared use facility with the City of Riverside, it does upon discussion with faculty/staff appear that the City take on a rental approach with the district rather than ownership. This perspective may be damaging if an incident occurs that results in the City pushing liability onto the district.</p>		
133		<p>The main entry at the Cosmetology Building (COSM) has experienced higher foot traffic of homeless people than the rest of campus due to location. Many times, they have entered or attempted to enter the building causing alarm to staff as often there are extenuating circumstances such as drugs involved. There is no</p>	<p>Install security electronics to provide monitoring of the building physically and visibly. Consider installation of a video intercom providing ability for remote release at the entry doors from the reception desk. The concerns regarding people with intent to cause harm wondering in from the street should be addressed. Replace</p>	4

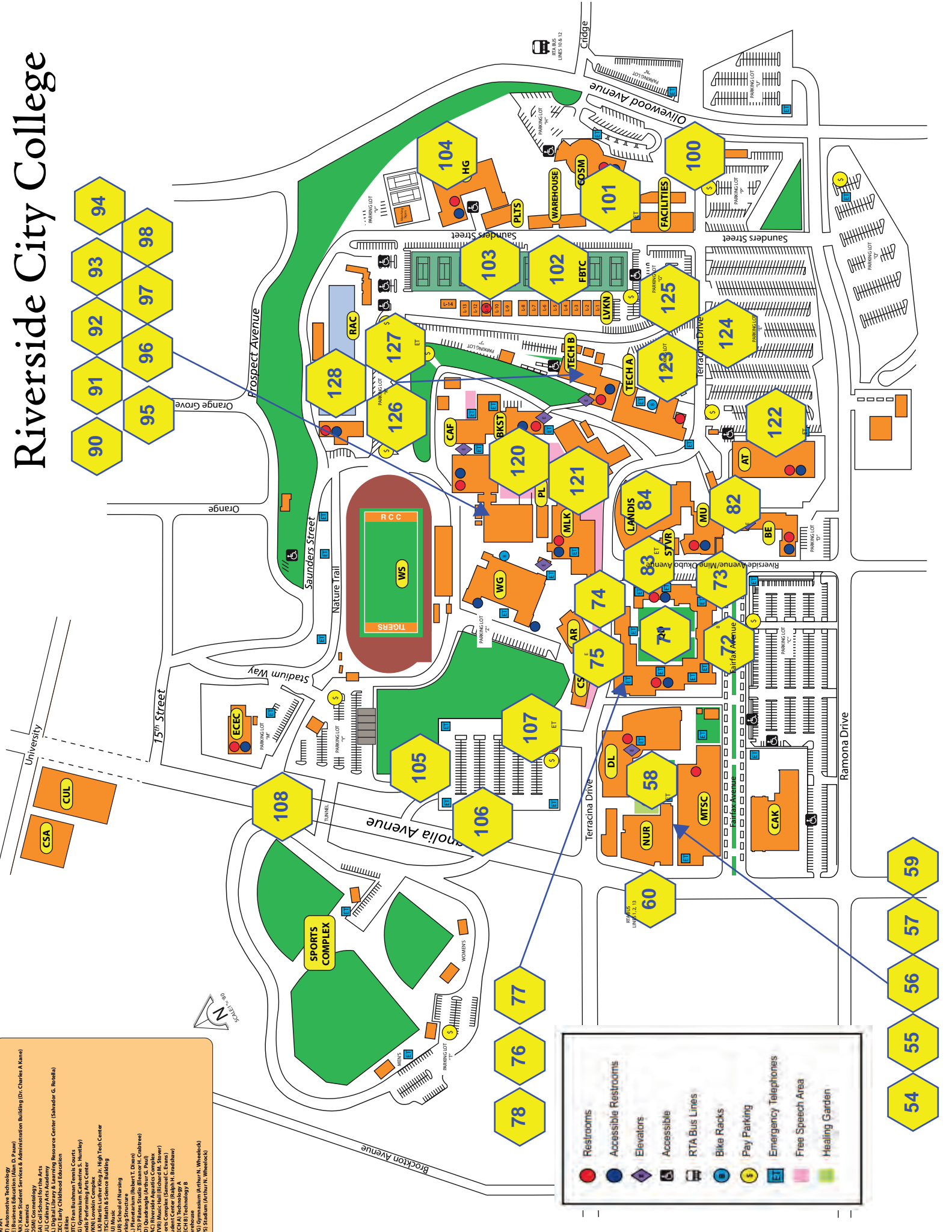
ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		<p>access control, intrusion detection, or video surveillance in use at this building. The emergency phone is a Trigon unit that is no longer available from the manufacturer. to the immediate right of the main entry there is restricted vehicle access down to the lower part of campus. There are no bollards or other vehicle barrier in place that would restrict unauthorized vehicle accessibility. There is no intercom that would allow for the main entry to be secured and authorized access be provided from the secure side via remote release of the entry doors. A legacy exterior horn/siren was observed with wiring left dangling from it. Unused legacy equipment should be removed to eliminate the perspective that if installed it is operable and has purpose.</p>	<p>the trigon all unit with a code blue emergency phone blue strobe combination wall mount enclosure. Demolish legacy exterior equipment that is no longer operational. Review the path of travel for vehicles and consider installation of removable bollards that would restrict unauthorized vehicle access.</p>	
134		<p>The main entry doors can be locked from the behind the main reception desk using the wall mounted switch which cuts power to the doors. This capability has recently been installed and is frequently used as the building encounters frequent interactions when people on drugs and affected by other issues. This is the only security measure in place that supports securing the facility during normal hours of operation, this is woefully inadequate based on staff/faculty shared experiences.</p>	<p>Provide a video surveillance monitor at the reception desk area that would real-time stream of exterior video surveillance cameras, providing general observation of activity.</p>	3

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
				
135		<p>Room 112 presents security challenges as the opening from the corridor has to remain unlocked at all times as an exit sign is located above the door indicating that it is in the path of egress. The door has a traditional classroom function lockset installed, and a lock block installed on the door frame. This is an example of an older building impacted by newer code regulations that present challenges to the security posture of the building. Maintaining a secured building envelope is essential to maintain security at this building when faced with built environment and code factors.</p>	<p>Review code requirements with the Fire Marshall, if possible secure the door from the corridor into the classroom mechanically.</p>	2
136		<p>Trees adjacent to the cosmetology parking lot require maintenance to eliminate lack of visibility. This is an area where homeless people have set up encampments. This issue was raised by the staff members within the cosmetology department, and they have</p>	<p>Perform landscaping maintenance, providing unrestricted visibility of activity at this area serving as a deterrent to persons who may be intending to set up an encampment.</p>	2

ID#	PHOTO	OBSERVATION	RECOMMENDATION	RISK
		concerns for their safety that should be acknowledged.		

Riverside City College

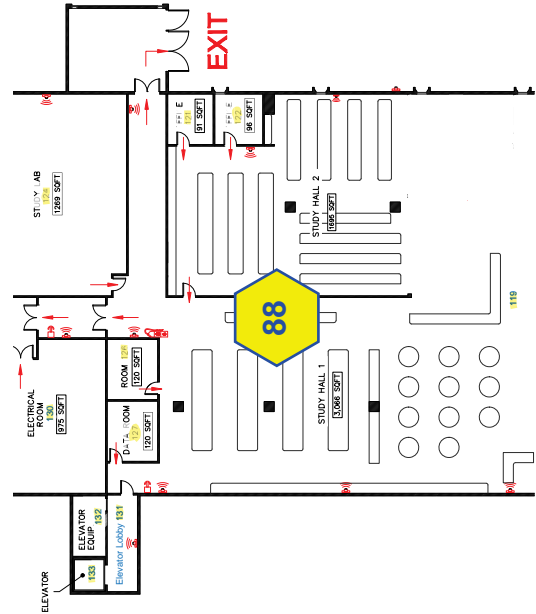
- 90
- 91
- 92
- 93
- 94
- 95
- 96
- 97
- 98



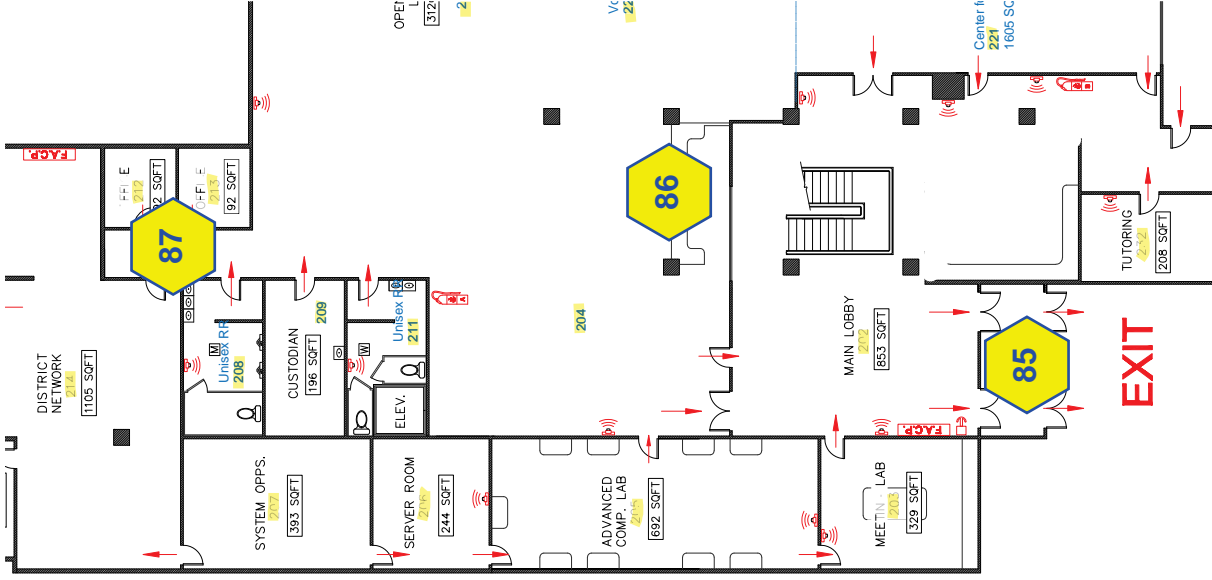
- 54
- 55
- 56
- 57
- 59

- (ART) Art
- (AT) Automotive Technology
- (BE) Business Education (Alan D. Pauer)
- (C) Child Development Center
- (CSA) Criminal Justice Services & Administration Building (Dr. Charles A. Kure)
- (CS) Cosmetics
- (COSM) Cosmetology
- (C) Call Center for the Arts
- (CUL) Culinary Arts
- (CUL) Culinary Library & Learning Resource Center (Salvador G. Bostela)
- (ECEC) Early Childhood Education
- (FBTC) Fran Bushman Tennis Courts
- (HG) Gymnasium (Catherine S. Hurley)
- (H) Health Services Center
- (LUVN) Loveland Complex
- (MLK) Martin Luther King Jr. High Tech Center
- (MUS) Music & Science Building
- (MUS) Music
- (NUR) School of Nursing
- (PA) Performance (Robert T. Dixon)
- (PLTS) Plastics Studio (Eleanor H. Crabree)
- (RAC) Restaurant (Arthur C. Papp)
- (STVR) Music Hall (Richard M. Stover)
- (S) Sports Complex (Samuel C. Bove)
- (T) Technology (L. Goldstein)
- (TECH A) Technology A
- (TECH B) Technology B
- (W) Wellness (Arthur N. Wheelock)
- (WS) Stadium (Arthur N. Wheelock)

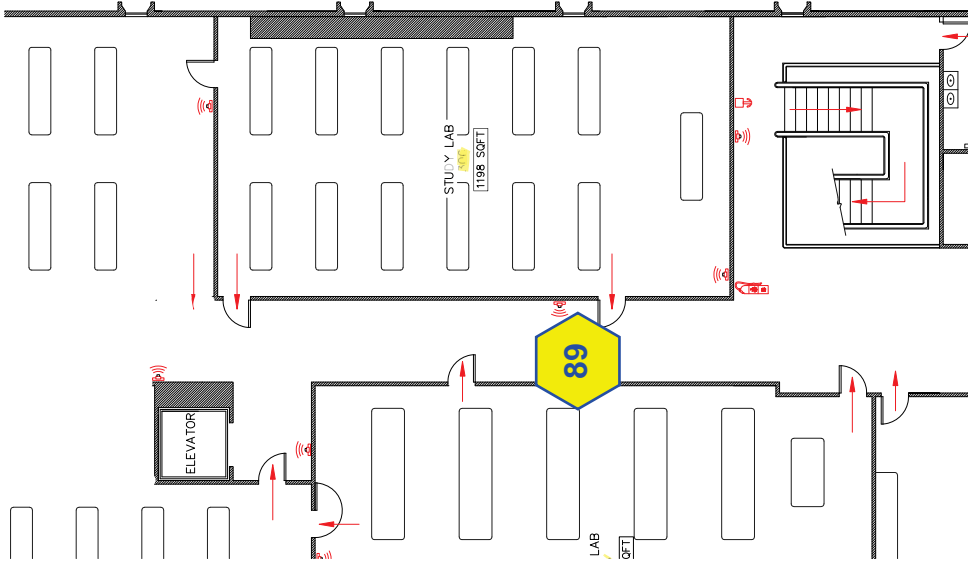
- Restrooms
- Accessible Restrooms
- Elevators
- Accessible
- RTA Bus Lines
- Bike Racks
- Pay Parking
- Emergency Telephones
- Free Speech Area
- Healing Garden

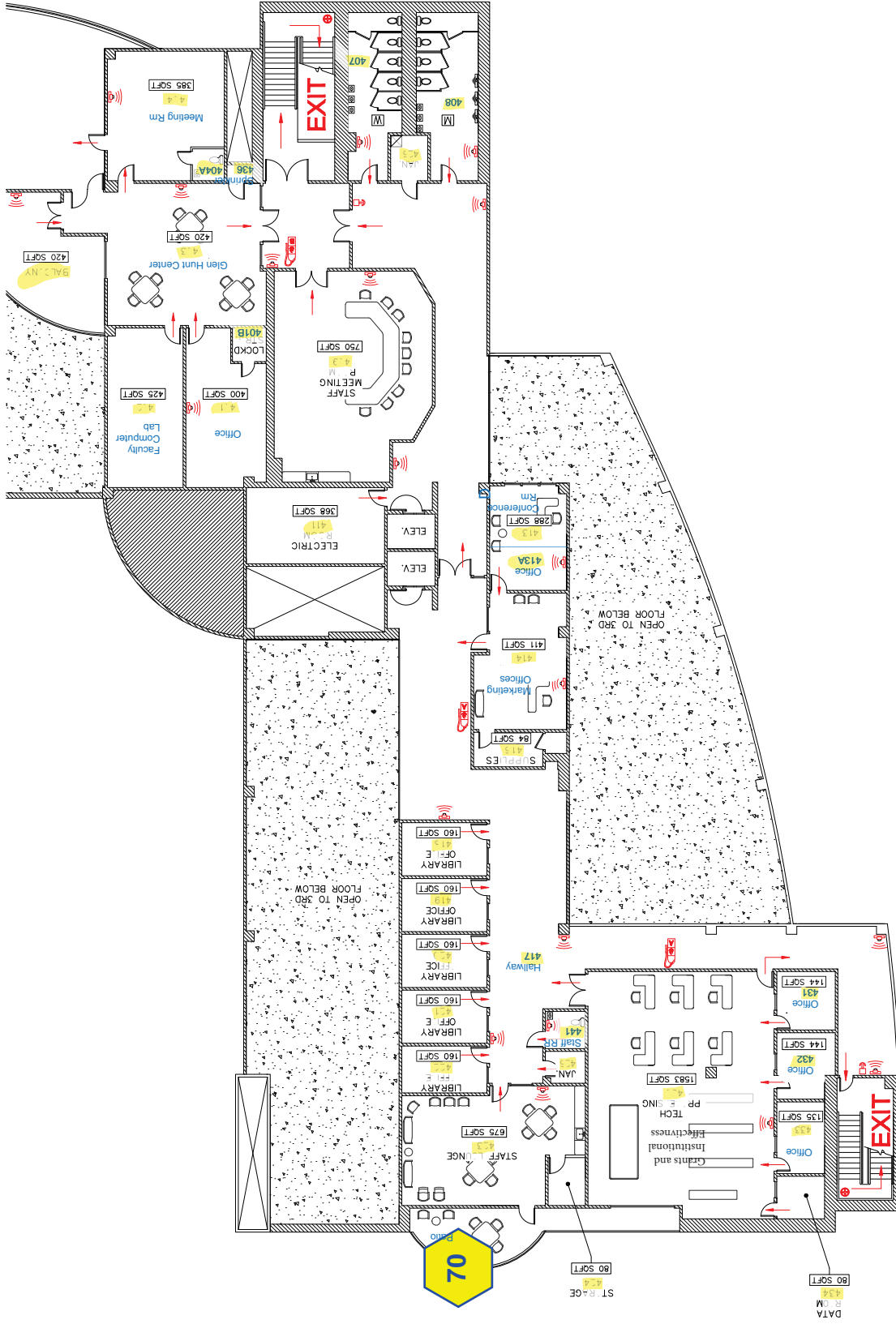


MLK FIRST FLOOR



MLK SECOND FLOOR





DL FOURTH FLOOR

BYLAWS OF THE RIVERSIDE CITY COLLEGE ACADEMIC SENATE

PREAMBLE

The Riverside City College Academic Senate (“RCCAS”) can propose, change, and amend its Bylaws by a majority vote of all of its members provided that (1) motions to amend the Bylaws must be proposed in writing and (2) two weeks must elapse between the making of a motion to amend and any action to adopt the motion.

ARTICLE I. MEETINGS & PROCEEDINGS

1. Regular RCCAS meetings will be scheduled in the Hall of Fame of the Bradshaw Student Center from 3:00 until 5:00 PM on the first and third Mondays of each month (contract holidays excepted) during the academic year, unless otherwise announced.
2. RCCAS meetings and faculty meetings called by the RCCAS are conducted under the parliamentary guidance of the most recent edition of Robert's Rules of Order, Revised.
3. Pursuant to the Ralph M. Brown Act [adds clarity about basis/rationale] space for public comments related to the purview of RCCAS will be included in each agenda.
 - The public may comment on items not included on the agenda during the “Public Comments” agenda item only.
 - Total time for public comments will be limited to 10 minutes.
 - Time limits for each individual speaker will be 3 minutes, unless there are several speakers in which case time may be reduced to ensure public comment is limited to 10 minutes.
 - According to Robert’s Rules of Order [per Counsel Dobyms, ref. to RR is unneeded] public comment is to be germane to the duties of the body, relate to current or new items for discussion and decision by the body, be respectful, and avoid the use of names or pejoratives.
 - RCCAS members may not discuss nor may they take action on public comments associated with items not on the agenda. If an RCCAS senator determines that the issue needs further discussion, the member may submit an agenda item dedicated to the issue at a subsequent meeting.
4. The RCCAS shall establish its own agenda by simple majority vote of the members present. The agenda must be established in accordance with State laws and regulations. Any member of the Riverside City College faculty may submit agenda items to the RCCAS. The established agenda may be abridged by majority vote or by consensus of the members present.
5. The RCCAS President will contact any Senator who misses three regularly scheduled meetings to assess the problem. If appropriate, the RCCAS President will contact the Senator's Department Chair regarding such absenteeism, with the hope of resolving the situation and avoiding departmental under-representation. Replacement of such absentee Senators may be necessary.

6. At its discretion, the RCCAS may authorize the RCCAS President to act on its behalf during the summer months. Wherever possible, action should be deferred until the Senate can meet and confer during the academic year.

ARTICLE II. ELECTIONS

1. Elections are conducted according to Article VIII of the Constitution.
2. The call for nominations shall be made at least three weeks in advance of the holding of an open faculty meeting which will constitute the closing of nominations.
3. In those years when the offices of President, Vice President, and Secretary-Treasurer are open for election, the College Academic Senate shall arrange in a timely manner through its committees for an open forum at which candidates for these positions may present themselves and their programs to the voting faculty.
4. Elections shall be conducted electronically or by campus mail in such a manner as to maximize the integrity of the electoral process.
5. The Nominations Committee shall establish the dates and times for distribution, collection, and counting of ballots so that the results can be posted immediately after votes are counted. The Nominations Committee will conduct the election in such a manner as to minimize the interference of the Spring Break with the election process.
6. The Nominations Committee shall request the Departments to hold elections for Department Senators and shall inform the Departments in a timely manner whenever a special need exists to fill a vacancy. Terms of office for Departmental Representatives to the Senate shall be for two (2) years with no limitation on the number of consecutive terms to which a departmental member may be elected as a Senator.
7. The Department representative elections shall be held as follows:

The following Departments shall elect representatives in odd-numbered years:

Applied Technology; Behavioral Sciences/Psychology; Business, Law, and Computer Information Systems; Communication Studies: English & Media Studies; History, Philosophy, Humanities, and Ethnic Studies; Library & Learning Resources; Life Sciences; Mathematics; Music; World Languages.

The following Departments shall elect representatives in even-numbered years:

Art; Chemistry; Cosmetology; Counseling/Student Activities; School of Education & Teacher Preparation; Economics, Geography, Political Science; Nursing; Dance and Theater; Physical Science; Kinesiology.

8. In the event that a departmentally-elected Senator is unable to serve due to extended medical leave, semester-abroad assignment, sabbatical leave, load-bank leave, other leave of absence, or is otherwise unable to regularly attend Senate meetings, the Department shall elect a replacement representative for the balance of the term and so indicate in Department minutes.
9. Where the Constitution requires election by majority vote, a runoff election will be held between the top two vote-getters. In some cases involving tie votes, a runoff between more than two candidates could occur.
10. [Review and discuss adding/revising this portion with Senator Weiler, RCCAS Associate Faculty Senator] According to Article VIII Section 5 of the Constitution, one Part Time Senator representing the part time faculty shall serve on the Senate. The Part Time Senator's term is for one year and begins on the first contract day of service in the academic calendar. According to Article III Section 2 of the Constitution, senators from the part time faculty shall be elected by the part time faculty. If for any reason the elected Part Time Senator is unable to serve, the RCCAS shall appoint to the position the eligible nominee who received the next highest number of votes.
11. Ballots and election results shall be kept on file in the Academic Senate office [update according to our current electronic tool?] and shall be available for review for 120 days.

ARTICLE III. RIVERSIDE CITY COLLEGE EDUCATIONAL PLANNING, LEADERSHIP COUNCILS, COMMITTEES AND WORKGROUPS

Section 1: Educational Planning Oversight Committee

- A. Pursuant to RCCAS's role in educational planning and budgeting under Title 5, §53200.10, the RCCAS President shall work with the President of Riverside City College to create an overarching strategic planning and operations structure for Riverside City College. The central structure shall be named the Strategic Planning Council and its primary input shall be the Educational Planning Oversight Committee ("EPOC"). The primary responsibility of the EPOC shall be to monitor institutional progress toward achieving college goals and to provide recommendations to the college president. EPOC also shall oversee and direct the general work of the Strategic Planning Leadership Councils ("SPLCs") and shall serve as the Accreditation Steering Committee when necessary.
- B. The Constitution and Bylaws of EPOC and the Riverside Strategic Planning Councils shall be ratified by the RCCAS. Any proposed changes to this document shall be brought before the RCCAS for consideration and ratification.
- C. The President of RCCAS shall accept nominations for faculty co-chair of EPOC, which will be brought to the RCCAS for deliberation and election. The President of Riverside City College shall choose an administrative co-chair for EPOC. These two will jointly oversee EPOC.

- D. The term of the faculty co-chair of EPOC shall be two years.
- E. The faculty co-chair of EPOC shall be regarded as an ex-officio, non-voting member of the RCCAS and shall provide regular reports the RCCAS.

Section 2: Strategic Planning Leadership Councils

- A. The Strategic Planning Leadership Councils (“SPLCs”) allow all members of the college community to participate in the decision-making process. Membership includes students, faculty, classified professionals, and administration. The SPLCs develop the college’s long-range plans, review and approve the Five-Year Comprehensive Program Review Plans in the areas for which they are responsible, monitor the specific activities of each unit and evaluate each unit’s Annual Assessment report, and link goals, vision, and processes for planning to resource allocation.
- B. The SPLCs, in accordance with their respective charges, shall determine when meetings are necessary in order to:
1. Develop and implement the college’s long-range strategic plans;
 2. Create integrated action plans to monitor, evaluate, and advance each unit’s action plans;
 3. Make recommendations to the Educational Planning Oversight Committee;
 4. Facilitate the dissemination of strategic planning information to the college community;
 5. Advance the implementation of college goals and targets; and
 6. Assess the progress each year the college makes to achieve its targets.
- C. The four (4) leadership councils are Student Access and Support (SAS); Teaching and Learning (TL); Resource Development and Administrative Services (RDAS); and Governance, Effectiveness, Mission and Quality (GEMQ).
- D. With the assistance of the faculty co-chair of EPOC, the RCCAS President shall accept nominations for the presiding faculty co-chairs of the SPLCs and bring them to the RCCAS for ratification. Appointments for presiding faculty co-chair and other faculty positions on the SPLCs shall be for two years; incumbents may be reappointed. To the degree possible, appointments shall be staggered terms. Members may be removed after three absences at the discretion of the constituent group. At the beginning of each academic year, the council shall provide the EPOC with a roster of voting members and other participating members.
- E. The faculty co-chairs of SPLCs shall represent their committees as ex-officio, non-voting members of the RCCAS and shall provide monthly reports to the RCCAS.
- F. The composition and charge of the SPLCs shall be articulated in the Constitution and Bylaws of EPOC and the Riverside Strategic Planning Councils.

Section 3: Standing Committees

- A. In general, committees perform work necessary for the policy and procedure recommendations of the SPLCs. Other committees are charged with addressing faculty issues under Title 5 §53200’s “10+1” and serve as stand-alone strategic and operational inputs, such as Curriculum. Committees that are tasked with academic issues (e.g.

Curriculum, Academic Standards, Associate Faculty) shall consist solely of faculty as voting members.

- B. Committees shall elect their chair in the spring prior to the term that begins in the fall. Faculty chairs of Committees shall be selected by the membership of the Committee and brought before RCCAS for confirmation. Committees who wish to do so may designate a faculty co-chair. The Chair of the Curriculum Committee shall serve as an *ex officio*, non-voting member of the RCCAS and shall provide reports as needed, at least once per semester, to RCCAS with the co-chairs of the Leadership Councils.
- C. Committees shall meet, at a minimum, once a month during the academic year. Committees may meet as part of District-wide committees where the Colleges of the District cooperate under the auspices of a Standing Committee of the District Academic Senate.
- D. The College President or designee shall identify an Administrator to serve as non-voting co-chair and to provide a liaison to the Administration on any Committee that has a committee that meets at the District level.

1. Curriculum Committee

- a. The Riverside City College faculty shall establish a Curriculum Committee, for the purposes of representing the faculty through the Senate to the Administration and to the Board of Trustees on all matters relating to any courses offered by the College. The Committee may freely utilize the expertise of all faculty in questions regarding specific courses, and shall direct special attention to the general issues of curriculum philosophy and development.
- b. The term of the chair of the Curriculum Committee shall be two years, beginning in the fall of even- numbered years. Should the Curriculum Committee choose a co-chair, the term shall commence in the fall of odd-numbered years.
- c. The Curriculum Committee shall be composed of Department representatives serving two-year terms of office. When new departments are established and their election year specified in the Bylaws or Bylaw revision is not synchronous with the time of scheduled elections or bylaws revision, a representative shall be elected to fill the length of the term remaining until the next scheduled election.
- d. In the event that a departmentally elected Curriculum Committee representative is unable to serve due to extended medical leave, semester- abroad assignment, sabbatical leave, other leave of absence, or is otherwise unable to regularly attend Curriculum Committee meetings, the Department shall elect a replacement representative for the balance of the term.

- e. The following Departments shall elect Curriculum representatives in odd-numbered years:

Applied Technology; Behavioral Sciences/Psychology; Business, Law, and Computer Information Systems; Communication Studies: English & Media Studies; History, Philosophy, Humanities, and Ethnic Studies; Library & Learning Resources; Life Sciences; Mathematics; Music; World Languages.

The following Departments shall elect Curriculum representatives in even-numbered years:

Art; Chemistry; Cosmetology; Counseling/Student Activities; School of Education & Teacher Preparation; Economics, Geography, Political Science; Nursing; Dance and Theater; Physical Science; Kinesiology.

- f. The RCC Articulation Officer is a voting member of the curriculum committee.
- g. Election of members of the Curriculum Committee shall take place by the full-time faculty members of the Departments in the same manner as Department Senators are chosen. Curriculum Committee members shall serve beginning on the first day of service of the academic year.

2. Academic Standards Committee

- a. The Riverside City College faculty shall have representatives on the District Academic Standards Committee. This committee will effectively function as a district committee with college representatives. RCCAS reserves the right to reformulate this committee as a college committee, if deemed necessary. Academic Standards exists for the purpose of recommending policy pertaining to student academic standards at Riverside Community College District and therefore, at Riverside City College. For example, the committee may recommend grading policies, withdrawal policies, degree standards, certificate standards, performance testing, remedial standards, transfer standards, non-transfer standards.
- b. The Academic Standards committee is composed of the curriculum chairs from each college in the district, the three Articulation officers from each college in the district, and one faculty member from each college's curriculum committee. As such, RCCAS is represented by its elected curriculum chair and another departmentally elected faculty from the curriculum committee, whose election is identified in the "Curriculum Committee" section of this document (3D1).

3. Departmental Leadership Committee

- a. The Riverside City College faculty shall recognize the Departmental Leadership Committee, which shall be tasked with articulating departmental and disciplinary issues, considering best practices for departmental operations, scheduling, and working with Academic Deans to assess and prioritize Comprehensive Program Review and five-year plans and other departmental and disciplinary matters.
- b. The members of the Departmental Leadership Council shall be constituted of department chairs as established in the prevailing “Agreement between Riverside Community College District and Riverside Community College District Faculty Association CCA/CTA/NEA.”
- c. Enrollment Management [coordinate with DLC/EM for language]

Section 4: Subcommittees

- A. Subcommittees perform work necessary for the policy and procedure recommendations of the SPLCs and Committees. Typically, Subcommittees work directly with the Committees to which they are attached. Subcommittees that are tasked with academic issues (e.g. Professional Growth and Sabbatical Leave, Course and Program Assessment, Faculty Program Review) shall consist solely of faculty as voting members. Subcommittees charged with ongoing, regular strategic and operational functions (such as Course and Program Assessment) shall have structures that mirror the college’s departmental structure.
- B. Subcommittees shall choose their chairs by majority vote at their first meeting, except for the chair of PGSL and the Faculty Development Subcommittee. This chair, the Faculty Development Coordinator, shall be determined by the subcommittee’s members, brought to the President of RCCAS and the President of Riverside City College and confirmed by the RCCAS. The faculty chairs of other Subcommittees shall be selected by the membership of the Subcommittee and brought before RCCAS for confirmation.
- C. Subcommittees shall meet, at a minimum, once a month during the academic year. Subcommittees may meet as part of District-wide committees where the colleges of the District cooperate under the auspices of a Standing Committee of the District Academic Senate.
- D. Each Subcommittee that has a District Academic Senate counterpart shall have an Academic Administrator to serve as non-voting co-chair and to provide a liaison to the Administration.

1. Professional Growth and Sabbatical Leave Subcommittee (PGSL)

- a. The RCCAS shall establish a Professional Growth and Sabbatical Leave Subcommittee, for the purpose of representing the faculty on all matters

relating to professional growth and sabbatical leave. This subcommittee will

effectively function as a district committee with college representatives. RCCAS reserves the right to reformulate this committee as a college committee, if deemed necessary.

- b. Two members of the RCC faculty will serve as voting members on the Riverside Community College District (RCCD) PGSL Committee, except when one of the members is serving as chair (see 4D1d). One voting member will be elected in even years and the other in odd years.
- c. The term of service for each member will be two years. In the spring, RCCAS officers will solicit nominations for this committee to be later ratified at an RCCAS meeting.
- d. The chair of the RCCD PGSL rotates amongst the three colleges each year. The chair of the committee does not have a vote during their year of service.
- e. RCC representatives on the Professional Growth and Sabbatical Leave Subcommittee shall liaison with the RCC Human Resources Committee of the Resource Development and Administrative Services Leadership Council.

2. Course and Program Assessment Subcommittee

- a. The RCCAS shall establish a Course and Program Assessment Subcommittee, for the purposes of representing the faculty in the Assessment Committee, known as the Riverside Assessment Committee or RAC, and to the Board of Trustees on all matters relating to ongoing academic course, program, and institutional level learning outcome assessment. The RAC may freely utilize the expertise of all faculty in questions regarding course, program and degree level assessment and shall direct special attention to the general issues of student learning outcomes assessment philosophy and development. The goal of the committee is to inform, instruct, and provide resources to faculty to facilitate discipline and department assessments.
- b. The RAC shall be composed of Department representatives serving two-year terms of office. When new departments are established and their election year specified in the Bylaws or Bylaw revision is not synchronous with the time of scheduled elections or bylaws revision, a representative shall be elected to fill the length of the term remaining until the next scheduled election.
- c. In the event that a departmentally elected RAC representative is unable to serve due to extended medical leave, semester-abroad assignment, sabbatical leave, other leave of absence, or is otherwise unable to regularly attend Assessment Committee meetings, the Department shall elect a replacement representative for the balance of the term.

- d. The following Departments shall elect Assessment representatives in odd-numbered years:

Applied Technology; Behavioral Sciences/Psychology; Business, Law, and Computer Information Systems; Communication Studies: English & Media Studies; History, Philosophy, Humanities, and Ethnic Studies; Library & Learning Resources; Life Sciences; Mathematics; Music; World Languages.

The following Departments shall elect Assessment representatives in even-numbered years:

Art; Chemistry; Cosmetology; Counseling/Student Activities; School of Education & Teacher Preparation; Economics, Geography, Political Science; Nursing; Dance and Theater; Physical Science; Kinesiology.

- e. Election of members of the RAC shall take place by the full-time faculty members of the Departments in the same manner as Department Senators are chosen. Assessment Subcommittee members shall serve beginning on the first day of service of the academic year.
- f. RAC shall liaison with the Governance, Effectiveness, Mission and Quality (GEMQ),

3. Academic Program Review Subcommittee

- a. The Riverside City College faculty shall establish an Academic Program Review Subcommittee for the purpose of working with academic units to complete Program Review and Plan (PRAP) document and Annual Unit Plan Updates or their equivalents and to bring this information to the Governance, Effectiveness, Mission and Quality (GEMQ).
- b. The Academic Program Review Committee shall be composed of Department representatives serving two-year terms of office. When new departments are established and their election year specified in the Bylaws or Bylaw revision is not synchronous with the time of scheduled elections or bylaws revision, a representative shall be elected to fill the length of the term remaining until the next scheduled election.
- c. In the event that a departmentally elected Academic Program Review Committee representative is unable to serve due to extended medical leave, semester- abroad assignment, sabbatical leave, other leave of absence, or is otherwise unable to regularly attend Academic Program Review Committee meetings, the Department shall elect a replacement representative for the balance of the term.

- d. The following Departments shall elect Academic Program Review representatives in odd- numbered years:

Applied Technology; Behavioral Sciences/Psychology; Business, Law, and Computer Information Systems; Communication Studies: English & Media Studies; History, Philosophy, Humanities, and Ethnic Studies; Library & Learning Resources; Life Sciences; Mathematics; Music; World Languages.

The following Departments shall elect Academic Program Review representatives in even- numbered years:

Art; Chemistry; Cosmetology; Counseling/Student Activities; School of Education & Teacher Preparation; Economics, Geography, Political Science; Nursing; Dance and Theater; Physical Science; Kinesiology.

- e. Election of members of the Academic Program Review Committee shall take place by the full-time faculty members of the Departments in the same manner as Department Senators and Curriculum representatives are chosen. Academic Program Review Committee members shall serve beginning on the first day of service of the academic year.
- f. The Academic Program Review Subcommittee shall liaison with the Governance, Effectiveness, Mission and Quality (GEMQ) leadership council.
- g. The chair of the Academic Program Review committee also serves on district committees for which program review is a focus area.
- h. The chair of the Academic Program Review committee shall attend EPOC meetings.

4. Distance Education Subcommittee

- a. The Riverside City College faculty shall establish a Distance Education Subcommittee to develop policies and promote practices that contribute to the quality and growth of distance education and bring these to the Teaching and Learning Leadership Council and Resource Development and Administrative Services Leadership Council (“RDAS”).
- b. The Distance Education Subcommittee shall be composed of six elected members serving two-year terms and representing the six divisions: Career and Technical Education; Counseling, Library and Learning Resources, and Academic Support; Fine and Performing Arts; Languages, Humanities and Social Sciences; Mathematics, Science and Kinesiology; Nursing. Three members shall be elected in even-numbered years and three shall be elected in odd-numbered years.

The following divisions shall elect representatives in odd-numbered years: Career and Technical Education; Fine and Performing Arts; Mathematics, Science and Kinesiology.

The following divisions shall elect representatives in even-numbered years: Counseling, Library and Learning Resources, and Academic Support; Languages, Humanities and Social Sciences; Nursing.

- c. The Distance Education Subcommittee will interface primarily with the Technology Resources Committee of Resource Development and Administrative Services Leadership Council.

5. Faculty Development Subcommittee

- a. The RCCAS shall establish a Faculty Development Subcommittee that seeks to encourage the professional development of faculty through collegially supported learning opportunities that share the vision and values of RCC.
- b. The Faculty Development Subcommittee shall be charged with creating the faculty development section of the Staff Development Plan.
- c. The Subcommittee shall consist of twelve voting members: ten full-time faculty members proportionally representing the academic divisions and one Associate (part-time) faculty member representing Associate faculty. The full-time faculty members shall be selected by their respective divisions via division elections, and the Associate faculty members shall be selected by the Associate Faculty via an Associate faculty election. The composition of the Subcommittee shall be as follows:
 - Languages, Humanities, and Social Sciences – three members
 - Career and Technical Education – two members
 - Mathematics, Science and Kinesiology – two members
 - Counseling, Library and Learning Resources, and Academic Support – one member
 - Fine and Performing Arts – one member
 - Nursing – one member
 - Associate (Part-Time) Faculty – one member

The above-mentioned faculty members shall serve as voting members on the Committee. Other non-voting faculty members may participate in the Committee planning and discussion.

The following divisions shall elect representatives in odd-numbered years: Career and Technical Education; Fine and Performing Arts; Mathematics, Science and Kinesiology.

The following divisions shall elect representatives in even-numbered years: Counseling, Library and Learning Resources, and Academic Support; Languages, Humanities and Social Sciences; Nursing.

- d. The Faculty Development Subcommittee shall liaison with the Human Resources Committee of the Resource Development and Administrative Services Leadership Council.

6. Course Materials Affordability Subcommittee

- a. The Riverside City College faculty shall establish a Course Materials Affordability Subcommittee (CMAC) to develop policies and promote practices that support efforts across the college related to Open Educational Resources (OERs), Zero Textbook Cost (ZTCs), and Low Textbook Cost (LTCs) materials in line with state legislation.
- b. The voting membership of CMAC shall be composed of six elected faculty members serving two-year terms and representing the six divisions: Career and Technical Education; Counseling, Library and Learning Resources, and Academic Support; Fine and Performing Arts; Languages, Humanities and Social Sciences; Mathematics, Science and Kinesiology; Nursing. Three members shall be elected in even-numbered years and three shall be elected in odd-numbered years.
 - The following divisions shall elect representatives in odd-numbered years: Career and Technical Education; Fine and Performing Arts; Mathematics, Science and Kinesiology.
 - The following divisions shall elect representatives in even-numbered years: Counseling, Library and Learning Resources, and Academic Support; Languages, Humanities and Social Sciences; Nursing.
- c. The CMAC will interface primarily with the Teaching and Learning Leadership Council

Section 5: Permanent Workgroups [delete--not consistent with Brown Act requirements]

~~A. Permanent Workgroups perform work necessary for the policy and procedure recommendations of the SPLCs and Committees and generally have a charge narrower than that of Subcommittees. Typically, Permanent Workgroups work directly with the Subcommittees to which they are attached. Permanent Workgroups that are tasked with academic issues shall consist primarily of faculty and shall have, at minimum, a majority of faculty as voting members.~~

~~B. Faculty chairs for Permanent Workgroups shall be chosen by the membership of the Permanent Workgroup.~~

Section 6: Temporary Workgroups

- A. Temporary Workgroups perform work necessary for the policy and procedure recommendations for strategic planning **or for other RCCAS initiatives**. Temporary Workgroups are given a specific, narrow charge by ~~superordinate~~ strategic planning groups **or RCCAS (typically Permanent Workgroups)** and may be convened or dissolved as necessary.
- B. Chairs of temporary workgroups shall be selected by the membership of the Temporary Workgroup and brought before the relevant strategic planning group **or RCCAS** for confirmation.

ARTICLE IV. ASSOCIATE FACULTY COMMITTEE

The Riverside City College faculty shall establish an Associate Faculty Committee, for the purpose of developing and representing the Associate Faculty issues to the RCCAS.

Additionally, as Associate Faculty are a valued part of the RCC faculty, any Associate Faculty member who wishes to broaden her/his experience by serving on a committee, subcommittee or workgroup other than the Associate Faculty Committee should contact the appropriate chair.

- A. The Associate Faculty Committee shall comprise five elected members serving two-year terms. Two shall be elected in even-numbered years and three shall be elected in odd-numbered years.
- B. The elected Associate Faculty Senator shall serve as chair on the committee and shall report to the RCCAS.



THE ACADEMIC SENATE FOR CALIFORNIA COMMUNITY COLLEGES

POSITION PAPER

Protecting the Future of Academic Freedom During a Time of Significant Change

ADOPTED FALL 2020



EDUCATIONAL POLICIES COMMITTEE 2019-2020

Nathaniel Donahue, ASCCC At Large Representative (Chair)

Stephanie Curry, ASCCC North Representative

Wendy Brill-Wynkoop, College of the Canyons

Julie Bruno, Sierra College

Angela Echeverri, Los Angeles Mission College

Manuel Vélez, San Diego Mesa College

TABLE OF CONTENTS

Introduction	1
Academic Freedom Defined	1
California Community College Changing Demographics	1
Academic Freedom and Free Speech	2
The Practice of Academic Freedom	3
Academic Freedom and Marginalized Communities	3
Freedom of Research and Publication	4
Freedom in the Classroom	5
Freedom for Public Discussion	6
Academic Freedom, Tenure, and Shared Governance for Full and Part-time Faculty	7
Academic Freedom and Tenure	7
Importance of Academic Senates and Unions Working Together	9
ASCCC Academic Freedom Survey	9
Academic Freedom Policies and Collective Bargaining Agreements	10
Academic Senate and Union Partnerships Regarding Academic Freedom	10
Protecting Academic Freedom Together: Effective Practices for Academic Senates and Unions	11
Other Considerations in Protecting Academic Freedom	13
Supporting the Academic Freedom of Colleagues	13
Academic Freedom and Systemwide Initiatives	14
Conclusion	15
Recommendations	16
Recommendations for Local Academic Senates:	16
Recommendations for Local Academic Senates in Collaboration with Union Colleagues:	16
References	17
Academic Freedom Resources	18
Appendices	18
Appendix 1: 1940 Statement of Principles on Academic Freedom and Tenure with 1970 Interpretive Comments.	18
Appendix 2: Academic Freedom Contract Language	18
Appendix 3: Executive Summary of ASCCC Academic Freedom Survey Results	18
Conclusions and Findings	23
Appendix 4: College of the Canyons Joint Understanding Between Senate and Union	23

INTRODUCTION

Academic Freedom Defined

Academic freedom is a fundamental concept that exists to ensure that institutions of higher education function for the public good and that colleges are constructed on the foundations of genuine trust. For over a century, members of The American Association of University Professors (AAUP) have been agile guardians, careful stewards, and erudite experts regarding the principle of academic freedom and its application in the faculty profession. In their historic “Statement on Academic Freedom and Tenure”¹ from 1940, the AAUP provides the definitive definition of academic freedom. Their major parameters state that the privilege and responsibility of academic freedom guarantees faculty “freedom in the classroom in discussing their subject,” “full freedom of research and in the publication of the results,” and the freedom from “institutional censorship or discipline” in their extramural speech. These three foundational principles protect discipline-based academic work from being corrupted or conducted for any other reason than the advancement of the public good.

California Community College Changing Demographics

When the AAUP first presented its “Statement of Principles on Academic Freedom and Tenure” in 1940, the community college campus was a different place in terms of student and faculty demographics. In fact, in the California junior or community colleges during that time, students of color—Latinx, Black, Native American, and Asian students—collectively made up less than half of the students enrolled in courses, while white students made up the largest group. Today, student makeup is quite different. In terms of ethnicity, for example, according to demographic data from the California Community Colleges Chancellor’s Office, students of color make up close to 65% of the student body, while white students represent 26%.

For faculty, the shift has not been as significant; however, changes in faculty demographics have been noticeable. Whereas in the 1940s faculty of color on college campuses were severely under-represented, today that representation improved slightly. In fact, in the California Community Colleges system today, tenured or tenure-track faculty of color comprise over 34% of the total faculty, while white faculty comprise over 58%; adjunct demographics are similar to tenure and tenure track. Similarly, demographics of faculty in relation to gender indicate a significant difference between 1940 and today. Whereas in the 1940s women made up only a small fraction of faculty on the campuses, today, according to the CCC Chancellor’s Office, 54% of all full-time tenured or tenure track faculty identify as female.

In reference to LGBTQ faculty and students, noticeable changes can be discerned despite the fact that little data currently exists in this area: while California’s AB 620 in 2011 encouraged community colleges to collect aggregate data on gender identity and sexual orientation, colleges are not required to do so. However, the passage of AB 620 as well as the establishment and increase of LGBTQ centers and alliances on college campuses certainly indicates positive trends in recognizing and creating space for LGBTQ

1 See Appendix 1 or <https://www.aaup.org/file/1940%20Statement.pdf>

faculty and students. In the CCCs alone, at least seventeen colleges have established LGBTQ safe-zones and alliances reflecting this trend.

All of this data indicates that today's college campus is vastly different in terms of diversity than it was in the 1940s when the AAUP presented its "Statement of Principles on Academic Freedom and Tenure" and raises important questions on the role of academic freedom in relation to these historically and currently marginalized communities. Colleges must consider whether a concept developed during a time when these communities were minimally considered—if at all—can apply equally to them today, as well as asking whether other considerations must be identified and addressed in regard to academic freedom given the changes in diversity of today's campus communities.

In considering these questions, the Academic Senate for California Community Colleges began a deep and sustained conversation on academic freedom. California community colleges are in a period of significant and systemic change. Faculty are engaging with and challenging each other to act in adopting culturally responsive teaching, in eliminating racism in all its forms—interpersonal, institutional, systemic—and in serving the whole student in ways that provide care and support as well as ensure a clear and direct path toward reaching an educational goal. At this time of change in the system, academic freedom may not be on the minds of many faculty. However, the principles of academic freedom are at the core of what faculty do as professionals in their classrooms, at their colleges, and in their communities and should not be forgotten or overlooked. The purpose of this paper is not to be the definitive word on academic freedom in the community college system; rather, it is to begin an exploration of what academic freedom means and how it should be protected and implemented in California's community colleges. This paper does not attempt to cover every aspect or nuance of academic freedom and its practice by faculty. Instead, this paper strives to lay a foundation to ensure that the principles of academic freedom remain strong and flexible to adapt to the changing dynamics in the California community colleges and in academia.

Academic Freedom and Free Speech

Sometimes the concept of academic freedom is confused with the Constitutional right to free speech,² presumably because both concepts regard principles of free expression. However, these rights differ both in those who possess them and in what they guarantee. Free speech is the right of every individual in the United States and is enshrined in the First Amendment. The freedom of speech protects a wide range of all-encompassing expression, including "the right to one's own opinion, however unfounded, however ungrounded, and extends to every venue and institution" (Scott, 2017). Furthermore, first amendment freedom of speech guarantees the right of all people in the United States to "the expression of their ideas, no matter how true or false they may be" (Dutt-Ballerstadt, 2018). Academic freedom is different and in many ways more restrictive. It is a right held by "educators in pursuit of their discipline," "addresses rights within the education contexts of teaching, learning, and research both in and outside the classroom for individuals at private as well as public institutions," and is "based in the pursuit of truth" (OAH Committee on Academic Freedom, n.d.). Whereas freedom of speech makes no requirement on the quality and type of expression, and indeed protects all forms of expression almost unconditionally, academic freedom

2 The specific wording of the first amendment, which includes freedom of speech, can be found at <https://constitution.congress.gov/constitution/amendment-1/#:~:text=Constitution%20of%20the%20United%20States&text=Congress%20shall%20make%20no%20law,for%20a%20redress%20of%20grievances>.

is very concerned with the quality and context of expression in order that it may contribute to both the academic discipline and the public good in “the pursuit of truth.” The absence of strong academic freedom policies and practices with protection of those practices leaves knowledge, teaching, learning, and students at risk of influence from outside forces that would like to harness the power and promise of education for motives focused on profit, social oppression, and the political suppression of critical thinking and informed dialogue.

Academic freedom is preserved and strengthened by the tenure process, which, like academic freedom, exists to ensure the public trust in institutions of higher education and the public servants who work in them. Without the professional security that tenure provides, faculty, their teaching, and their research may be subject to influences that possess motivations misaligned with the stewardship of the public good and the pursuit of truth.

THE PRACTICE OF ACADEMIC FREEDOM

The practice of academic freedom assures that the conditions are created for the unfettered advancement of knowledge in the pursuit of truth. It promises that the contributions faculty make to their disciplines, in teaching and in research, are uncorrupted by outside forces who would seek to harness the power of education, and the students who seek it, for their own self-centered ends or to maintain the status quo. Such motivations may not necessarily be in alignment with the creation of an informed citizenry and an educated society. Academic freedom is required so that faculty professionals who teach and research are protected from external forces that might try to influence the development of culture, science, and knowledge in order to serve any interest other than the intellectual, socioeconomic, and socioemotional advancement of students through the attainment of an education. Although it is often misunderstood and nefariously cast as a principle that exists to advance the political opinions or interests of a learned elite, on the contrary, academic freedom is a requisite that protects against the political, economic, moral, and intellectual corruption of institutions of higher education. It does not give teachers the right to impose their personal or political views upon students, to ignore college or university regulations, to defend any form of professional incompetence, or to teach outside their subject matter or the official course outline of record. Academic freedom is a fundamental concept that exists to ensure that institutions of higher education function for the public good and assures that colleges are constructed on the foundations of genuine trust.

ACADEMIC FREEDOM AND MARGINALIZED COMMUNITIES

Considerations of diversity in a campus community typically refer to a demographic perspective that reflects the diverse nature of the community and its students. In this sense, discussions such as hiring, retention, and support of faculty are important but are only indirectly related to academic freedom. Instead, academic freedom, as defined by the AAUP, relates to freedom of research and publication, freedom in the classroom for faculty to discuss their subjects, and freedom to have public discussions. In this sense, while issues of retention and hiring are certainly important in terms of diversity, discussions

on academic freedom in relation to these communities should focus more on issues related to these three freedoms in the context of faculty's institutional and professional experience.

Freedom of Research and Publication

The demographic change on campuses not only created a more diverse population, but it also introduced diverse concepts and ideas into an academic environment that has been and continues to be dominated by patriarchal euro-centric paradigms. This trend is evident especially in California community colleges, where the growth of ethnic studies-related programs has continued to increase yearly, as has the introduction of general education courses with emphases on marginalized communities. These are strong indicators of the growing influence of a diverse faculty on the academic discourse in the colleges, which is certainly a benefit for students. In many ways, academic freedom has played an important role in ensuring that this influence could exist. Not only is this fact evident in the establishment of ethnic studies programs, but perhaps even more so in the proliferation of publications and research related to marginalized communities. Scholars in recent years have placed great emphasis on researching communities that were once ignored by academia. Scholarly texts on Black, Latinx, women's, and LGBTQ history are beginning to fill college bookshelves as faculty exercise their freedom to research what they believe to be relevant. This proliferation in publications leads to more exposure of these communities and ideas to students as faculty introduce them in their curriculum and, as indicated in extensive research, provide students with a stronger education.

However, this change has not come without resistance. Because the focus on historically marginalized communities must also include an analysis of the forces responsible for that marginalization, research from these communities tends to challenge and undermine long-held academic paradigms that are based on patriarchal and Eurocentric notions and that still dictate academic discourse and curriculum today. For this reason, the introduction of this research tends to come with controversy and resistance. Today, this controversy can be found in the focus on "decolonization of curriculum," a growing academic concept that attempts to challenge the long-established traditional notions of pedagogy and academics by focusing on paradigms that replace and undermine those established by colonization. As discussions of decolonization grow, attempts to dismiss it can also be found. Opponents of the concept dismiss it as political activism or attempts at political correctness and as such remove it from the realm of academic discourse. This trivialization often serves to discourage faculty from pursuing research in these areas and to protect patriarchal and Eurocentric paradigms. In this sense, academic freedom serves as a function counter to what it is intended to serve. Rather than encouraging the freedom to research and publish, academic freedom can be used by those opposed to new paradigms and focuses as a means of protecting traditional approaches and discouraging faculty from marginalized communities from introducing concepts that may address and improve the campus experience for all faculty and students.

Another area in which academic freedom in research and publication has been an engine for progress and the common good is medicine and the sciences. The ability to challenge prevailing wisdom or the status quo has always been instrumental to significant advances in human understanding of the natural world. In many cases, new ways of thinking and free inquiry have initially been vehemently opposed by other scholars and society at large, but when the truth eventually prevailed, it led to monumental

paradigm shifts. Whether it involved challenging creationism, geocentrism, Lamarkism, spontaneous generation, or the etiology of infectious diseases, history is replete with cases in which the pursuit of knowledge and progress have been hindered by a lack of academic freedom in research and publication. For example, Ignaz Semmelweis' groundbreaking studies in the 1840s on the cause of childbirth fever in obstetric wards and the importance of handwashing in its prevention were met with such ridicule, hostility, and resistance from his fellow physicians that he was forced to leave his job (Davis, 2015). An untold number of women and children tragically and unnecessarily lost their lives as a result of the initial suppression of his findings. While today most people understand that handwashing is essential in preventing the spread of infectious disease, making doctors wash their hands was at one point in history considered a radical notion. This example shows a case in which academic freedom could have protected not only Semmelweis' job and right to publish his research but also the pursuit of knowledge and the common good.

Freedom in the Classroom

The second principle identified by the AAUP recognizes the freedom of faculty to teach and discuss the subjects they choose within the classroom. This freedom is of particular relevance for students in that it directly relates to their right to learn, a right also specifically identified by the AAUP. This freedom has allowed for faculty to introduce concepts to their students that are free from political, administrative, or monetary influence, and recently allowed for a more diverse perspective in regard to marginalized communities within the classroom. By introducing concepts and topics into an academic setting such as a classroom, faculty in essence validate those concepts and topics as worthy of academic discourse for their students. In cases where topics reflect the students' own background and cultural history, this acknowledgement serves to validate their own presence on campus and give them a sense of belonging.

Examples of this progress have become increasingly common since the beginning of the early 1900s. One such example is the publication of the book *With His Pistol in His Hand* by Dr. Americo Paredes. This book focused on the role of the Corrido in Mexican-American society in the early 1900s and represented thorough research on the Mexican-American experience in the Southwest at that time. Dr. Paredes' work became the first extensive research on Mexican-American folklore in the United States and served as the foundation for continued research in that culture. Today, Paredes' book is still widely read and discussed in college courses throughout California, as are other topics related to Mexican-American and other ethnic cultures. Such teachings help to give students a well-rounded and comprehensive perspective on their societies and a stronger education overall, and once again academic freedom has served as a driving force in their proliferation. In fact, today the number of courses that focus on marginalized communities continues to increase, and this increase can be directly attributed to academic freedom.

Unfortunately, as with the freedom to research and publish, the freedom to teach and introduce these new concepts and topics can come with resistance as well. This resistance may come in the form of lack of administrative support at the campus level or even from within the faculty itself. Once again, because the study of and the teaching about marginalized communities necessarily includes a discussion of the conditions that cause their marginalization, these concepts are often challenged and discouraged by

those who embrace more traditional paradigms and trivialized by those who do not see such study as fitting within the traditional paradigms of academia. In his article “How and Why is Academic Freedom Important for Ethnic Studies,” David Palumbo-Liu echoes this idea:

Ethnic studies is particularly vulnerable to denials of or infringements upon academic freedom not only because the kinds of knowledge it generates are considered peripheral to the core mission of the university, but also because its modality of opposition and contestation wins it no friends among most administrators (Palumbo-Liu, 2016).

At the administrative level, this resistance may mean that courses with focus on such communities are given less priority and as such, are offered less than other courses. It may also mean less priority on the hiring of faculty who emphasize these communities in their research. Resistance may also come from faculty who oppose these new concepts and perspectives. This resistance often appears as challenges to the academic integrity of the concepts or topics and thus may remove them from the protection of academic freedom.

Freedom for Public Discussion

Perhaps no other freedom as defined by the AAUP has been more impacted by modern developments than the freedom for public discussion. Twenty-first century technological advancements have enabled a level of public discourse never even imaginable in the 1940s. This advancement certainly comes with myriad advantages in regard to freedom of expression for everyone; however, in regard to academic freedom, it has added layers of complexities and challenges. These advancements have played an important role in the evolution of college curriculum and the inclusion of new and dynamic pedagogical approaches that challenge long-standing academic norms. While social media sites such as Twitter and Facebook can serve as volatile spaces for discussion, they offer a level of discursive engagement for marginalized communities that did not previously exist.

Unfortunately, the volatility of social media can also threaten academic freedom. The case of Steven Salaita, a newly-hired tenured faculty member of the Indian Studies department at the University of Illinois in Urbana-Champaign, is a clear example of this threat. In 2014, Salaita criticized U.S. policy in regard to Israel and Palestine via social media platforms. This criticism, along with growing public demands, drove the University of Illinois to rescind its offer of employment (Flaherty, 2015). This case exemplifies the complexities of academic freedom in this social media age. While Salaita’s comments were not made in an academic environment nor in a peer-reviewed article, they still fall under the definition of public discussion and as such might be categorized as academic freedom. However, given that social media is a recent phenomenon, it is something that deserves and necessitates stronger focus.

ACADEMIC FREEDOM, TENURE, AND SHARED GOVERNANCE FOR FULL AND PART-TIME FACULTY

In the California Community Colleges system, college governance must adhere to Education Code and Title 5 regulations, as codified in local policies, procedures, and practices.³ Academic senates spend an extraordinary amount of time and energy ensuring that governance, as it relates to academic and professional matters, follows the law and is effective for the institution. However, in focusing on the effectiveness of college governance, faculty tend not to pay as close attention to academic freedom as the “indispensable requisite for unfettered teaching and research in institutions of higher education” (American Association of University Professors, n.d. a) nor to the role that tenure affords in safeguarding the protections of academic freedom. The principles inherent in both academic freedom and tenure not only provide protections for the profession but also delineate the responsibilities faculty have to their disciplines, the students, the institution, the public, and each other. Since the strength of the protection of academic freedom and tenure affects all faculty, it is an issue that should be of deep concern for both academic senates and collective bargaining units. As such, these organizations must work together to ensure the vitality and survival of academic freedom and tenure within the system. In recognizing how important academic freedom is to the profession, faculty must also recognize that its very existence is inextricably dependent upon tenure. As confirmed by AAUP, a principle purpose of tenure is to safeguard academic freedom (American Association of University Professors, n.d. b).

Academic Freedom and Tenure

In 1988, Assembly Bill 1725 (Vasconcellos)⁴ included mention of the importance of full-time faculty to the community colleges. This sentiment was later included in Title 5 regulation as an aspirational goal—frequently referred to as the 75/25 goal—for 75% of instruction to be performed by full-time tenured or tenure track faculty. The goal is also referenced in Education Code §87482.6, which details the use of the faculty obligation number and funding in an effort to make progress toward the goal. However, regardless of the support of both Education Code and Title 5, the community college system has never met the goal, and this situation has critical implications for tenure, academic freedom, and governance, particularly regarding collegial consultation.

Tenure in the California community colleges is threatened and has been for many years; consequently, so has academic freedom. Funding for the California Community Colleges system has always been unstable, dependent upon state allocations, property taxes, and political will. Overall, the state allocation per student has remained flat over time,⁵ and with the 2018 alteration in the system funding formula to include performance-based funding, district budgets have gone through considerable change both in the amount of funding colleges receive and in the predictability of that funding. That uncertainty has only been exacerbated in recent times by the economic fallout caused by a global pandemic.

3 For more information, see the ASCCC Local Senates Handbook at <https://www.asccc.org/papers/handbook2015>.

4 The text of AB 1725 (Vasconcellos, 1988) is available at <https://edsource.org/wp-content/uploads/old/ab1725.PDF>

5 According to the California Community Colleges Chancellor’s Office Data Mart, per student funding remained relatively flat over the previous ten years as of 2019.

Historically, in response to these financial uncertainties, community colleges have increasingly relied on part-time faculty who by the very nature of their employment status are easily hired or terminated depending on fluctuations in funding, student headcount, course offerings, and staffing needs. Additionally, the community colleges system continues to rely on the faculty obligation number (FON) to determine the minimum number of full-time faculty per district as required by the Board of Governors. Unfortunately, the FON has remained relatively unchanged since its inception in 1989. Rather than making progress toward the 75/25 goal, districts tend to use the FON as a ceiling rather than the floor to benchmark the number of full-time faculty to hire each year, resulting in stagnant and even decreasing numbers of tenure-track faculty in the CCC system (Bruno, et.al., 2018). Currently, the community colleges have approximately 16,451 full-time faculty and 37,918 part time faculty.⁶ Thus, approximately 70% of faculty within the system are part-time and do not have the protections of tenure status. The static number of full-time tenured faculty and the necessary corollary of reliance on part-time faculty has left colleges in a weakened position regarding tenure. This weakening of tenure adversely affects the protection and benefits of academic freedom, including participation in governance, for all faculty.

The numbers of full- and part-time faculty have a direct impact on academic freedom and the ability of faculty and colleges to engage in robust participatory or shared governance. Although academic senates represent all faculty in academic and professional matters, regardless of employment status, and all faculty share a commitment to fulfilling academic and professional responsibilities outlined in Title 5 §53200, structural barriers exist for part-time faculty to participate in the governance of their colleges. One of the fundamental purposes of tenure is to protect a faculty member's ability to speak truth to power without retribution. Although the strength of this protection varies widely across the system because it is frequently dependent upon college policies, contract language,⁷ and due process procedures, the fact that tenure provides some protection for full-time faculty is a privilege not experienced by part-time faculty. Even if some, albeit weaker, form of protection extends to part-time faculty through seniority, rehire rights, or due process rights under law, the pervasive threat of losing employment still exists, and processes to grieve the encroachment into areas of academic freedom are minimal or nonexistent. This threat has a chilling effect on participation in college governance.

Furthermore, part-time faculty are frequently unable to participate in governance due to their workload, and, if they are able, they are rarely compensated for governance work. This burden was recognized as far back as 1988 in a passage from AB1725 (Vasconcellos):

If the community colleges are to respond creatively to the challenges of the coming decades, they must have a strong and stable core of full-time faculty with long-term commitments to their colleges. There is proper concern about the effect of an over-reliance upon part-time faculty, particularly in the core transfer curricula. Under current conditions, part-time faculty, no matter how talented as teachers, rarely participate in college programs, design departmental curricula, or advise and counsel students. Even if they were invited to do so by their colleagues, it may be impossible if they are simultaneously teaching at other colleges in order to make a decent living (Assembly Bill 1725, Vasconcellos, 1988, Section 4.b).

6 Data from the Fall 2019 semester according to the California Community Colleges Chancellor's Office Data Mart.

7 See Appendix 2

If the part-time faculty who form the majority of faculty within the community college system are uncompensated or unable to participate in college governance, then that burden falls solely on the full-time faculty.

IMPORTANCE OF ACADEMIC SENATES AND UNIONS WORKING TOGETHER

Faculty organizations must collaborate to improve the status of academic freedom, tenure, and governance within the community colleges system for the benefit of faculty, students, and the community at large. Although a local academic senate may at times find itself at odds with interests of or positions taken by the local collective bargaining unit or union, these conflicts, potentially pitting one faculty group against another, do not serve faculty or the institution well. Both academic senates and faculty unions must be clear regarding their purview in governance of the college, and all will benefit when both entities respect each other's purview and continue to collaborate on shared interests and issues. Academic freedom is one shared issue that is frequently neglected by both academic senates and unions. Although many colleges have academic freedom policies and some unions have negotiated language into their local contracts, faculty may nevertheless face direct threats to academic freedom.

ASCCC Academic Freedom Survey

In a 2019 Academic Senate for California Community Colleges survey on Academic Freedom,⁸ sent through local academic senate presidents, more than 50% of those responding indicated that their contracts did not contain a robust policy on academic freedom with due process for both full- and part-time faculty. In another finding, approximately 47% of respondents indicated that their academic senates had not created a strong statement that defined the parameters of academic freedom for faculty. Only about half of respondents agreed that their local academic freedom statement and board policy were widely distributed and easily accessible to all faculty. More than 90% of respondents indicated that faculty did not receive training on academic freedom at their campuses.

Respondents identified several topics that had been debated with regard to academic freedom on their campuses, including textbook selection, teaching methodology, implementation of statewide initiatives, faculty evaluations, grading policies, freedom of speech in and out of the classroom, and curriculum offerings. More than 13% of those responding reported that outside organizations had been involved with the surveillance and censoring of college faculty or others on their campus. The survey results support the need for collective bargaining units and academic senates to work together to protect academic freedom, tenure, and shared governance for all faculty.

⁸ See Appendix 3.

Academic Freedom Policies and Collective Bargaining Agreements

As of 2020, eighty-three faculty collective bargaining agreements are established within the California Community Colleges system, yet only forty have some mention of academic freedom. Many simply include reference to the local district board policy on academic freedom, noting that faculty have a contractual obligation to observe all policies. When academic freedom is included in the collective bargaining agreement, this language is the default. However, listing academic freedom in collective bargaining agreements not as a right of faculty but rather as another task that faculty must absorb as part of their workload is insufficient. The 2019 ASCCC Survey on Academic Freedom revealed that only 45% of respondents agreed or strongly agreed that their contract contained a robust policy on academic freedom and due process for academic freedom for both full-time and part-time faculty.

In order to protect academic freedom, collective bargaining agreements should strive to assert the unique right of academia, particularly in the area of tenure, evaluation, and due process. The agreements must acknowledge academic freedom as a professional right of the faculty and reference the standard definition in the 1940s AAUP statement of principles. In the AFT Guild Local 1931 2020-2022 collective bargaining agreement with San Diego Community College District, faculty rights to academic freedom permeate the document not only by acknowledging the 1940 Statement of Principles, but also by specifically calling out the right to faculty privacy, including use of email, and a noted expectation of the faculty to protect students' academic freedom. This collective bargaining agreement stands out in particular as an example incorporating the importance of academic freedom in the faculty evaluation process (Faculty Bargaining Unit, 2020).

Academic Senate and Union Partnerships Regarding Academic Freedom

Academic senates must recognize that unions can be a powerful force to help combat the erosion of academic freedom and ensure faculty certain protections under academic freedom. According to the 2005 AAUP Academic Unionism Statement, being a member of a union includes a number of benefits that complement the benefits of being a member of the academic senate, including the following:

- Unions enable faculty and other members of the academic community, who would be powerless alone, to safeguard their teaching and working conditions by pooling their strengths.
- Unions make it possible for different sectors of the academic community to secure contractual, legally enforceable claims on college administrations, at a time when reliance on traditional advice and consent has proved inadequate.
- Unions may provide members with critical institutional analyses—of budget figures, enrollment trends, and policy formulations—that would be unavailable without the resources provided by member dues and national experts.
- Unions increase the legislative influence and political impact of the academic community as a whole by maintaining regular relations with state and federal governments and collaborating with affiliated labor organizations.

- Unions reinforce the collegiality necessary to preserve the vitality of academic life under such threats as de-professionalization and fractionalization of the faculty, privatization of public services, and the expanding claims of managerial primacy in governance.

In support of academic senates and unions working together, the 2005 AAUP statement goes on to say that “[s]trong senates and strong union chapters can work together to preserve and protect academic freedom on campus. Together, they establish the institutional terrain and precedents on which individual rights are defined, defended, and sometimes adjudicated” (American Association of University Professors, 2005).

Protecting Academic Freedom Together: Effective practices for Academic Senates and Unions

In order to represent faculty effectively, local academic senates and unions should strive to create a collegial and collaborative relationship, one that delineates and respects the unique role of each entity and strives to support both. Faculty are best served when both the academic senate and the union are strong. A faculty divided against itself undermines academic and professional standards, impairs working conditions, and damages the educational integrity of the institution.

In defining this relationship, faculty need to be aware of the different approaches used by academic senates and unions. Negotiation is the primary tool used by unions to draft the contract between faculty and the district in order to determine the conditions of employment, such as but not limited to wages, working hours, overtime, safety conditions, class size, evaluation procedures, due process for discipline, seniority, academic calendar, sick leave, retirement benefits, health benefits, professional development requirements, grievance methods, and participation in college service activities. On the other hand, academic senates develop policies and processes regarding academic and professional matters through collegial consultation with the board of trustees or its designee. Collegial consultation is defined as either relying primarily upon the advice and judgment of the academic senate or reaching mutual agreement (Title 5 §53200). Although very different, the two approaches work as counterbalances to each other. When the union and the academic senate collaborate, the benefits of both approaches are clearly visible in the strengthening of the faculty as a whole and support the design of mutually beneficial college policies and processes that are culturally informed and responsive to the dreams, goals, and needs of a diverse student body.

To reach a mutually beneficial state, the academic senate and the union may wish to create a joint agreement or memorandum of understanding to clearly define the role and purview of each entity and the working relationship between the two. This agreement may best be developed when the entities are not in conflict or stressed in dealing with major concerns.⁹ A collegial relationship between the academic senate and the union is critical so that each entity may represent faculty within its purview. A written agreement is one way to ensure the effectiveness of working together, particularly as a road map to continue collaboration in the future through the change of faculty leaders of both bodies.¹⁰

9 See Appendix 4.

10 For more information on establishing a collegial working relationship between the academic senate and the union, see the 1996 ASCCC paper *Developing a Model for Effective Senate/Union Relations* at https://www.asccc.org/sites/default/files/publications/senate_union_relations_1996_0.pdf.

As academic senates and faculty unions establish strong working relationships, one of the first items on the collective agenda should be to review the institution's policy on academic freedom and ensure that it is codified in the contract to protect both full- and part-time faculty. Academic senates should take the lead on defining the parameters of academic freedom—e.g. instructional methodology, textbook selection, syllabi, etc.—through resolution, policy, or other means as dictated by local process. These parameters will help to support and inform contractual agreements on academic freedom negotiated by the union. The union should negotiate protections for both full- and part-time faculty, including due process for violations and ensuring the faculty evaluation process does not encroach on academic freedom.

Once the union has negotiated robust protections for academic freedom into the collective bargaining agreement, professional development for faculty is crucial. Again, this area is one where the academic senate and the union should collaborate. Training should be provided for all faculty—part-time, tenure-track, and tenured—on academic freedom and participating in the evaluation process. Special consideration should be given to how faculty evaluate faculty in the classroom, both on-ground and on-line. The tenure process for faculty in community colleges relies heavily on student evaluations. According to one recent study of tenure-track faculty, the factors most associated with higher student ratings were the attractiveness of the faculty member and the student's interest in the class; the factors most associated with lower student ratings were course difficulty and whether student comments mentioned an accent or a teaching assistant. Not surprisingly, faculty tended to be rated more highly when they were young, male, white, in the humanities, and held a rank of full professor (Murray, et.al, 2020).

Faculty should be aware of the scope of evaluations and how to ensure that the evaluation does not infringe upon the academic freedom of a faculty member being evaluated. If one faculty member has questions about what another faculty member is doing regarding anything that is within the faculty member's academic freedom parameters as established by the academic senate, those conversations must be collegial and nonevaluative. They should be professional, with the goal of understanding different ways of teaching, and should in no way be brought up during the evaluation process. Ultimately, the academic senate and the union should work together to ensure that all faculty understand and protect the academic freedom rights and responsibilities of all faculty.

Once protections are in place, a determination should be made regarding who or what will be the arbiter in the case of a perceived violation of a faculty member's academic freedom. As an academic and professional matter, these potential violations should go before a duly constituted—appointed or elected—faculty committee to review the situation and recommend action. The committee should be composed of members who are knowledgeable of both the parameters of academic freedom as determined by the academic senate and the contract and due process for violations of those parameters. Committee members should undergo regular training on the academic freedom parameters and due process to remain current and effective. Such a committee may act as a source of campus expertise on academic freedom.

OTHER CONSIDERATIONS IN PROTECTING ACADEMIC FREEDOM

Other areas on which the academic senate and union should collaborate regarding academic freedom include providing joint union and academic senate professional development and training for faculty and specifically for academic senate leaders. In the 2019 ASCCC Survey on Academic Freedom, an overwhelming majority of respondents, 93%, indicated that their colleges provided no professional development on academic freedom for faculty. Ideally, professional development regarding academic freedom should be provided for all faculty locally, including implementing local board policies and procedures in light of the parameters set by the academic senate and the contract obligations negotiated by the union. Academic senates, with the assistance of union colleagues, should review their own procedures and those of their standing committees for possible constraining of or incursion into areas of academic freedom.

Finally, academic senates and unions should educate administrators, board members, and the campus community as well as the larger community on the importance of academic freedom, tenure, and shared governance as the most effective methods of ensuring the integrity of the institution and ensuring the public trust.

Supporting the Academic Freedom of Colleagues

Faculty can take many actions to strengthen and support the academic freedom of their colleagues across the community college system and indeed across the nation. First, local academic senates can encourage the creation and adoption of a supportive board policy delineating the parameters of academic freedom on each campus. Further, each local senate can create its own statement regarding the practice of academic freedom at a variety of levels, including the generation of new curriculum and retirement of older courses, professional development, the implementation of diverse and innovative pedagogies in the individual classroom, evaluations, and grading policy, among others.

Sometimes supporting the academic freedom of colleagues at the department level can become fraught, especially because individual academic freedom can find itself in tension with local departmental policies, procedures, and the collective decision-making process. Decisions regarding common course materials and textbooks can often intersect with individual academic freedom. For example, a faculty member might desire to use open educational resources (OER) for a course that makes use of a common print textbook chosen by the department. The department may have chosen a common text so that students do not have to purchase additional course materials or for various other reasons. Often departmental questions regarding the quality and rigor of materials can inspire intense feelings among discipline faculty who are passionate about their subjects and student success. As long as the faculty are choosing course materials that are in alignment with the course outline of record, individual faculty can make a legitimate argument that they have the right to choose their own course materials under the tenets of academic freedom.

In a situation such as a conflict over course materials, robust discussion should take place within the department, and ideally a consensus solution could be found. The same type of discussion may be had for student learning outcomes, another area in which departments adopt common standards and policies across courses. Another intra-faculty issue that can sometimes cause consternation among colleagues regarding the practice of academic freedom is grading policies. Academic freedom allows faculty to evaluate student work in a manner that they best see fit in order to teach the material. This point is an especially important point to acknowledge, because commentary surrounding grading policies can often appear in evaluations of faculty work within the classroom by peers during the tenure process. Some faculty equate rigor with a standard bell curve, while others believe that courses may be rigorously designed in ways in which most students master the material and earn high marks. In either case, while colleges and departments have a right to set and maintain academic standards, simply using grade distribution in the evaluation of faculty work would infringe upon the parameters of academic freedom. Ideally, local academic senates and communities of practice within departments would set suggested guidelines for the evaluation of student work and grading policies but not act as bodies of surveillance and enforcement.

One of the best and most important ways faculty can support the academic freedom of their peers is for local academic senates along with their union colleagues to develop robust professional development opportunities regarding the parameters and practice of academic freedom. If faculty and colleges do not establish a clear understanding of the boundaries and responsibilities attendant on the privilege of academic freedom, a clear delineation of why academic freedom is practiced in service of students and the public good in order to create a foundation of trust in public institutions of education, and a sound articulation of how the tenure process is the essential basis of academic freedom, the future of academic freedom will teeter in jeopardy.

Academic Freedom and Systemwide Initiatives

The California Community Colleges system is constantly engaged in a process of continuous improvement in order to educate the whole student in the best way possible. Faculty are always interrogating their pedagogies, improving their services, and innovating change so that they can be as effective as possible. The dialogue of continuous improvement may take place at a variety of levels in which faculty take the lead: the individual classroom, the department, or on local and statewide academic senate committees.

Sometimes, change knocks on the door from outside the system and is encouraged by entities who have different prerogatives and intentions than faculty. However, because academic freedom exists to protect education for the public good and to ensure that students are allowed free inquiry, it must be the faculty, whose expertise is teaching and student engagement, who lead the effort to improve the quality and delivery of the education they deliver. Faculty must be properly resourced so that they may have the time and space to genuinely collaborate with administrators and system partners in a meaningful way that reflects the best principles of participatory governance and collegial consultation. Faculty, engaged in a constant process of improvement, welcome the suggestions, expertise, and help of enthusiastic partners in student success because faculty believe that through the process of collaboration and shared governance, colleges can achieve the best results, and they require financial support in order to achieve

the mission of the system for students and for the state. Most of all, the faculty of the California Community Colleges system understand that they are living in the “fierce urgency of now” (King, 1963) and will not be satisfied until all students are achieving their self-stated goals and the system is achieving equitable results. However, when the goals of system partners intersect with the academic and professional responsibilities of faculty as delineated in Title 5 §53200, academic freedom may become threatened.

Many well-intentioned system initiatives and grant-funded projects can inadvertently encroach upon the boundaries of academic freedom, and faculty must therefore not only be vigilant but step up and take ownership of the change management process in a meaningful way. Resources must be devoted to faculty with pertinent expertise regarding whatever innovation is being implemented or project is at hand, and faculty must have access to robust professional development that ensures that they become leaders and agents of systemic change.

Specifically in the area of curriculum development, many pratfalls can be avoided in order to protect the integrity of academic freedom. An example is the recent implementation of Assembly Bill 705 (Irwin, 2017), a well-intentioned law designed to support students completing transfer level math and English in their first year, and ESL in three years. Nowhere did the law necessarily recommend curricular changes; it was intended to change the placement of students in courses in order to increase their timely success. However, a variety of external organizations campaigned and applied significant political pressure to eliminate entry-level courses, and many community college districts followed this direction, often over the objections of faculty. In such a situation, because each campus in the system is so different and because student bodies are so diverse in their needs and composition, careful and intentional collaboration is instead needed to make certain that all of the implications for equity and student success have been considered on each individual campus as everyone is engaged with systemic change. For these reasons, reform and redesign movements like guided pathways must be firmly grounded in faculty leadership as outlined in Education Code and Title 5. Specifically, curriculum development, student learning outcomes, the organization of programs within clusters, and the ways that colleges deliver counseling services, among many others matters, require a strong process of collaboration grounded in principles of shared governance in order to preserve the essential tenets of academic freedom.

CONCLUSION

Academic freedom is an essential aspect of education that protects the free exchange of ideas and should be at the forefront of academic senate conversations. The opportunities afforded by academic freedom, including areas of teaching, research, and extramural speech, are at the cornerstone of free education. Because faculty members have the right to teach, research, and speak freely on their areas of expertise, community dialogue is expanded and equitized. Academic freedom allows new ideas and marginalized stories to be brought to the forefront of academic discussion. The tenure structure is essential to providing faculty the safety and protections to fully embrace their academic freedom. Academic senates and faculty unions should work together to create processes, procedures, and contract language to protect all faculty's academic freedom. They should also support and train faculty in the facets of academic freedom through multiple and systematic professional development opportunities.

RECOMMENDATIONS

Recommendations for Local Academic Senates:

1. Local senates should create a statement on academic freedom, in addition to local board policy, that delineates the specific issues and parameters of academic freedom for faculty.
2. Local senates should provide consistent and ongoing professional development for full- and part-time faculty and senate leaders—curriculum, program review, policy chairs, senators, etc.—in the principles and tenets of academic freedom, including onboarding new faculty.
3. Local senates should work to review, revise, and strengthen shared governance processes, policies, and procedures in relation to academic freedom so that shared governance protects dissenting opinions in the decision-making process.

Recommendations for Local Academic Senates in Collaboration with Union Colleagues:

1. Local senates should work with union colleagues to develop due process around violations or perceived violations that involve academic freedom issues, including a duly constituted—appointed or elected—faculty committee to review and recommend action.
2. Local senates should collaborate with union colleagues on codifying the protection and parameters of academic freedom in contract in light of faculty evaluations, curriculum, online instruction, dual enrollment, open educational resources, guided pathways, and other relevant issues.
3. Local senates should work with union colleagues to train faculty on engaging in faculty evaluations in light of academic freedom.
4. Local senates should clearly delineate and provide justification for adjunct faculty participation in shared governance in order to support union efforts to negotiate appropriate compensation.
5. Local senates and union colleagues should review AAUP resources and recommendations.

REFERENCES

- American Association of University Professors. (2005). *Academic Unionism Statement*. Retrieved from American Association of University Professors website: <https://www.aaup.org/academic-unionism-statement>.
- American Association of University Professors. (n.d. a). *Advancing Academic Freedom*. Retrieved from American Association of University Professors website: <https://www.aaup.org/our-work/protecting-academic-freedom>.
- American Association of University Professors. (n.d. b). *Tenure*. Retrieved from American Association of University Professors website: <https://www.aaup.org/issues/tenure>.
- Assembly Bill 1725, Vasconcellos. (1988). Retrieved from <https://edsources.org/wp-content/uploads/old/ab1725.PDF>.
- Bruno, J., Carroll, C., Dowd, B.A., Duncan, W., Hansen, R., Mahler, J., . . . Wyse, J. (2018). *The 50% Law and the Faculty Obligation Number: An Updated Proposal*. Retrieved from <https://www.asccc.org/sites/default/files/50-percent-Law-and-FON-Updated-Proposal.pdf>.
- California Education Code §87482.6 Retrieved from [http://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=EDC§ionNum=87482.6#:~:text=\(1\)%20In%20computing%20the%20percentage,instruction%20taught%20by%20full%2Dtime](http://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=EDC§ionNum=87482.6#:~:text=(1)%20In%20computing%20the%20percentage,instruction%20taught%20by%20full%2Dtime).
- Davis, R. (2015). The Doctor Who Championed Hand-Washing And Briefly Saved Lives. *Shots: Health News From NPR*. January 12. Retrieved from <https://www.npr.org/sections/health-shots/2015/01/12/375663920/the-doctor-who-championed-hand-washing-and-saved-women-s-lives>.
- Dutt-Ballerstadt, R. (2018). When Free Speech Disrupts Diversity Initiatives: What We Value and What We Do Not. *Journal of Academic Freedom* 9. Retrieved from <https://www.aaup.org/sites/default/files/Dutt-Ballerstadt.pdf>.
- Faculty Bargaining Unit with San Diego Community College District. (2020). Retrieved from <https://aftguild.org/wp-content/uploads/2020/01/SDCCD-Faculty-CBA-01-01-20-through-06-30-22.pdf>.
- Flaherty, C. (2015). Censure Threat. *Inside Higher Ed* April 28. Retrieved from <https://www.insidehighered.com/news/2015/04/28/aaup-slams-u-illinois-handling-steven-salaita-case>.
- King, M.L. Jr. (1963). I Have a Dream, Address Delivered at the March on Washington for Jobs and Freedom. *The Martin Luther King, Jr. Research and Education Institute*. Stanford University. Retrieved from <https://kinginstitute.stanford.edu/king-papers/documents/i-have-dream-address-delivered-march-washington-jobs-and-freedom>.
- Murray, D., Boothby, C., Zhao, H., Minik, V., Bérubé, N., Larivière, V., & Sugimoto, C. (2020) Exploring the personal and professional factors associated with student evaluations of tenure-track faculty. *PLoS ONE* 15(6). Retrieved from <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0233515>.
- OAH Committee on Academic Freedom. (n.d.) Academic Freedom Guidelines and Best Practices. *Organization of American Historians*. Retrieved from <https://www.oah.org/about/governance/policies/academic-freedom-guidelines-and-best-practices/>.
- Palumbo-Liu, D. (2016, January). Why and How Is Academic Freedom Important for Ethnic Studies? *Journal of Ethnic Studies* 19 (1): 101-103. Retrieved from https://www.researchgate.net/publication/298209175_Why_and_How_Is_Academic_Freedom_Important_for_Ethnic_Studies.
- Scott, J. W. (2017). On Free Speech and Academic Freedom. *Summer 2017 Bulletin*. American Academy of Arts & Sciences. Retrieved from <https://www.amacad.org/news/free-speech-and-academic-freedom>.
- Title 5, California Code of Regulations, §53200. Retrieved from <https://govt.westlaw.com/calregs/Document/I6EED7180D48411DEBC02831C6D6C108E?transitionType=Default&contextData=%28sc.Default%29>.

ACADEMIC FREEDOM RESOURCES

- Academic Freedom in the 21st-Century College and University: Academic Freedom for All Faculty and Instructional Staff.* (2007). American Federation of Teachers. Retrieved from <https://www.aft.org/sites/default/files/academicfreedomstatement0907.pdf>.
- American Association of University Professors. (1970). *1940 Statement of Principles on Academic Freedom and Tenure.* Retrieved from American Association of University Professors website: <https://www.aaup.org/report/1940-statement-principles-academic-freedom-and-tenure>.
- American Association of University Professors. (1988). *Statement on Academic Government for Institutions Engaged in Collective Bargaining.* Retrieved from American Association of University Professors website: <https://www.aaup.org/report/statement-academic-government-institutions-engaged-collective-bargaining>.
- American Association of University Professors. (2015). *Policy Documents and Reports.* Eleventh edition. Retrieved from American Association of University Professors website: <https://www.aaup.org/reports-publications/publications/redbook>.
- Messier, J. (2017). Shared Governance and Academic Freedom: Yes, This Is Union Work. *National Education Association.* Retrieved from https://www.nea.org/assets/docs/TA2017S_Messier.pdf.
- Reichman, H. (2015). Professionalism and Unionism: Academic Freedom, Collective Bargaining, and the American Association of University Professors. *AAUP Journal of Academic Freedom* Vol. 6. Retrieved from https://www.aaup.org/sites/default/files/Reichman_0.pdf.
- Reichman, H. (2019). *The Future of Academic Freedom.* John Hopkins University Press.

APPENDICES

Appendix 1: 1940 Statement of Principles on Academic Freedom and Tenure with 1970 Interpretive Comments

Insert from <https://www.aaup.org/file/1940%20Statement.pdf>

Appendix 2: Academic Freedom Contract Language

Insert from https://drive.google.com/file/d/1N2vwAQRdLFSyDn6xTM5f1KffLpibh1_8/view?usp=sharing

Appendix 3: Executive Summary of ASCCC Academic Freedom Survey Results

- Based on a recommendation from the Educational Policies Committee, the ASCCC conducted a statewide online survey on Academic Freedom during January of 2020.
- Responses were submitted during a two-week period between 1/14/20 to 1/25/20.
- The survey contained a total of 13 questions.
 - Two questions obtained information on college demographics and faculty role.
 - Nine questions were multiple choice or True/False and are summarized below.
 - Two questions were open ended:
 - Question 7: How often do your faculty receive professional development regarding Academic Freedom?

- Question 10: If a faculty member on your campus believes their Academic Freedom has been violated, what happens? Has your senate been involved with the creation of a due process?

- The survey elicited 66 responses from faculty representatives at 39 different colleges.
 - A total of 37 colleges submitted a single response to the survey.
 - Two institutions, Taft and LA Southwest Colleges, had multiple responses, 12 and 15 respectively.

Figure 1 summarizes responses to the following two statements (Survey Questions 3 & 4):

1. Our local Academic Senate participated in the creation and/or review of a **Board Policy** regarding Academic Freedom
2. Our **Academic Senate** has created a strong **Statement** regarding Academic Freedom that defines the parameters of Academic Freedom on our campus.

Figure 1: Local Academic Senate Participated in Creation of Board Policy or Senate Statement on Academic Freedom

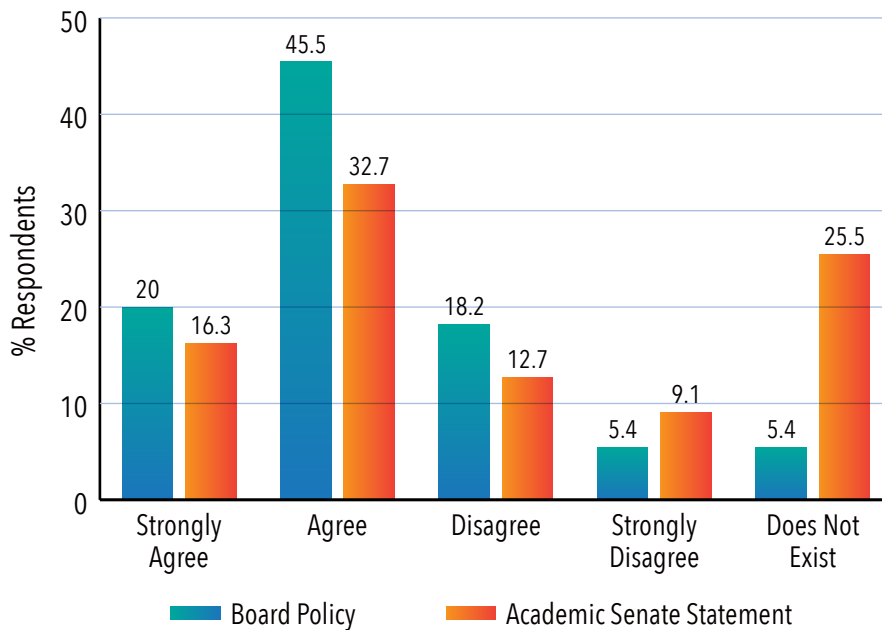


Figure 2 summarizes responses to the following statement (Survey Question 5):

Our Academic Freedom statement and Board Policy are widely distributed and easily accessible to full-time and part-time faculty.

Figure 2: Widely Distributed and Easily Accessible Board Policy and Senate Statement on Academic Freedom

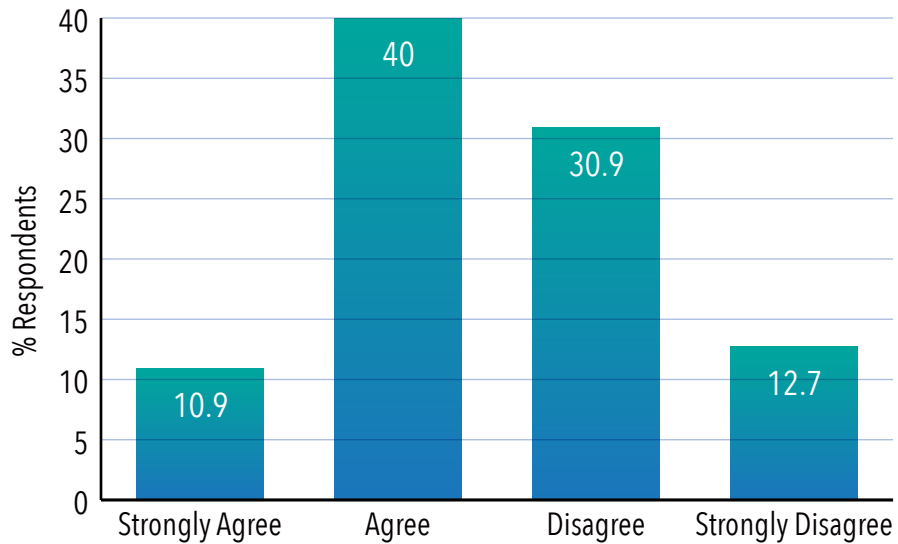


Figure 3 summarizes responses to the statement (Survey Question 6):

Faculty receive professional development training regarding Academic Freedom on our campus

Figure 3: Faculty Receive Training on Academic Freedom

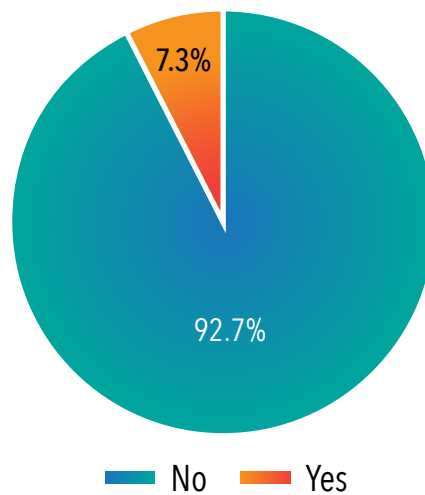


Figure 4 summarizes responses to the statement (Survey Question 8):

Our contract contains a robust policy on Academic Freedom and due process for Academic Freedom for both full-time and part-time faculty:

Figure 4: Contract Contains Robust Policy on Academic Freedom and Due Process for All Faculty

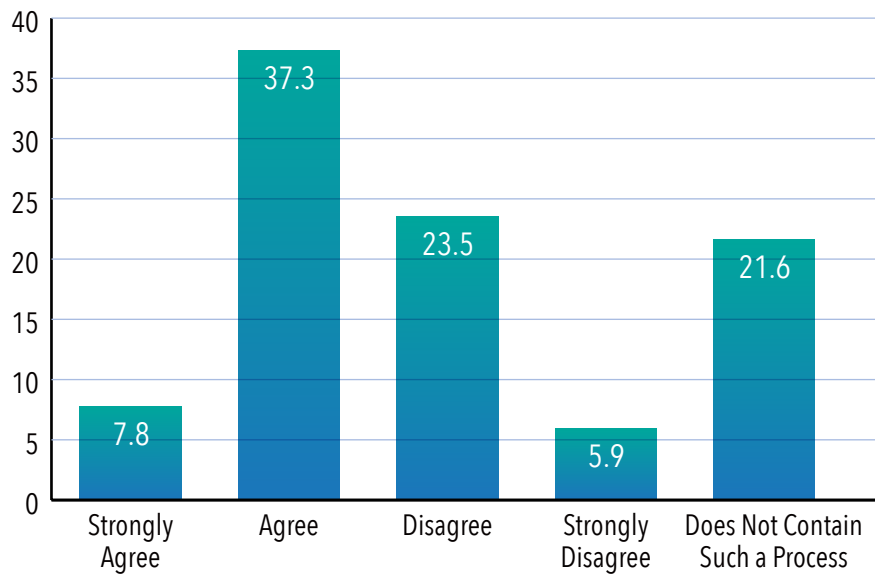


Figure 5 summarizes responses to the statement (Survey Question 9):

Please indicate if any of the below subjects have been debated on your campus with regards to how they intersect with Academic Freedom (you may select more than one).

Figure 5: Topics Debated with Regards to Academic Freedom

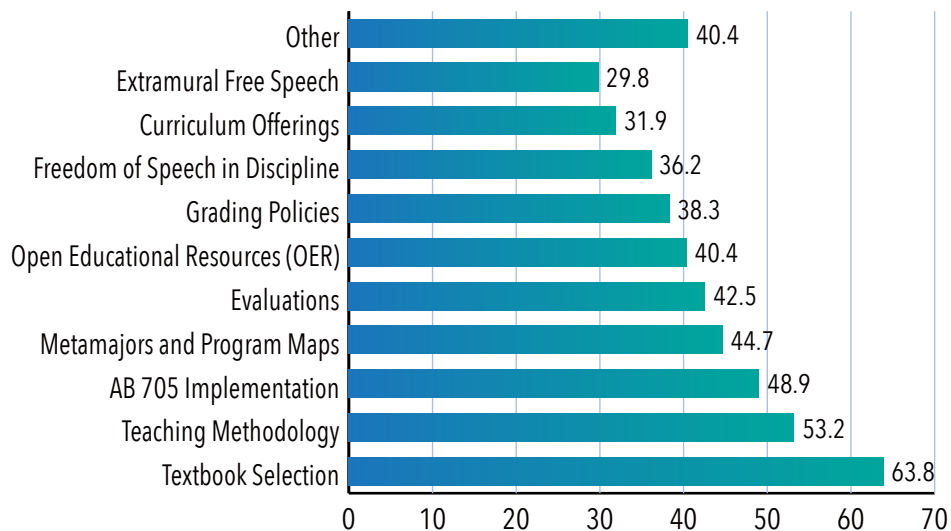


Figure 6 summarizes responses to the following question (Survey Question 11):

Have outside organizations been involved with the surveillance and censoring of college faculty and/or administrators and staff on your campus? If so, please explain.

Figure 6: Surveillance and Censuring by Outside Organizations

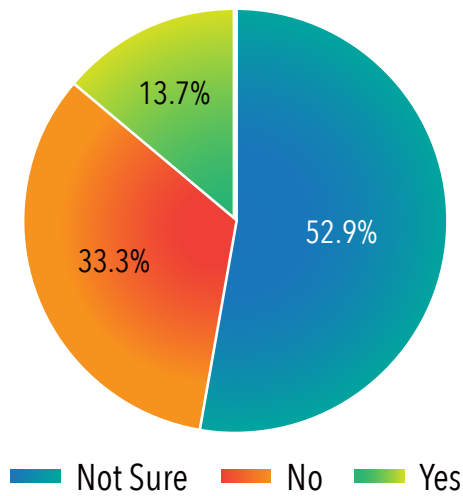


Figure 7 summarizes responses to the following question (Survey Question 12):

Has the ratio of hours taught by full-time tenure track faculty fallen in the past five years when compared with the number of hours taught by part-time faculty on your campus?

Figure 7: Has the Ratio of Hours Taught by Full-time Faculty Dropped in Last 5 years?

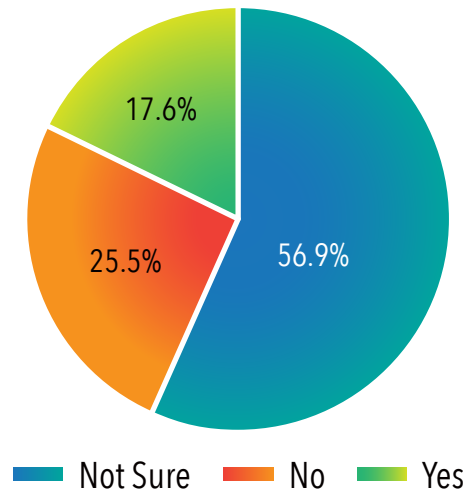
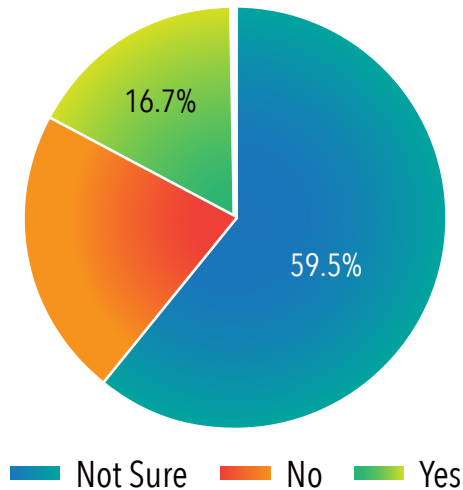


Figure 8 summarizes responses to the following question (Survey Question 13):

If the ratio of hours taught by full-time tenure track faculty has fallen when compared to hours taught by part-time faculty, do you believe this has had any effect on the security of academic freedom on your campus? If so, please explain.

Figure 8: Has a Lower Ratio of Hours Taught by Full-time Faculty Affected Academic Freedom on Your Campus?



Conclusions and Findings

- **Board Policy on Academic Freedom:** 65% respondents agreed or strongly agreed that the senate had participated in Board Policy on Academic Freedom, 24% disagreed or strongly disagreed, and 5% indicate the Board had no Academic Freedom Policy.
- **Senate Statement on Academic Freedom:** 49% respondents agreed or strongly agreed that the senate had created a statement on Academic Freedom, 21.8% disagreed or strongly disagreed, and 25.5% indicate the Senate had no Academic Freedom statement.
- **Widely Distributed and Easily Accessible Academic Freedom Policy and Statement:** 50.9% agreed or strongly agreed, while 43.6 disagreed or strongly disagreed.
- **Training on Academic Freedom:** Over 92.7% of respondents indicated faculty did not receive training on Academic Freedom, only 7.3% reported faculty received training on this topic.
- **Contract Policy and Due Process for Academic Freedom:** 45.1% respondents agreed or strongly agreed that their contract had a robust policy on Academic Freedom, 29.4% disagreed or strongly disagreed, and 21.6% indicate their contract had no Academic Freedom policy.
- Topics debated with regards to Academic Freedom:
 1. Textbook selection: 63.8%
 2. Teaching methodology: 53.2%
 3. AB 705 implementation: 48.9%
 4. Faculty Purview in Metamajors and Program Maps Creation: 44.7%
 5. Evaluations: 42.6%
 6. Open Educational Resources Implementation or Prohibition: 40.4%
 7. Grading policies: 38.3%
 8. Freedom of Speech in Discipline: 36.2%
 9. Curriculum offerings: 31.9%
 10. Extramural Free Speech: 29.8%
 11. Other: 40.4%
- **Surveillance or censoring by outside organizations:** 13.7% reported surveillance or censoring by outside groups, 33.3% reported none, and 52.9% were not sure.

Appendix 4: College of the Canyons Joint Understanding Between Senate and Union

Insert from https://www.canyons.edu/_resources/documents/administration/academicssenate/documentspage/academicssenatestandingrulesandstatements/JointCollaborativeconsultationUnderstandingJCCUsigned.pdf



 This publication is printed on recycled paper. Please recycle your copy when done.

Academic Senate for California Community Colleges
One Capitol Mall, Suite 230, Sacramento, CA 95814
916.445.4753 www.asccc.org

©2020 Academic Senate for California Community Colleges



ASCCC Common Course Numbering Phase III Summer Convenings and Survey Opportunities

Faculty nominations within each discipline or course below for ratification at RCCAS on Monday, April 7. [see highlighted nominees]

Any disciplines that missed the window but would still like to put forward nominees should contact President Scott-Coe before Friday, April 11.

Background: The ASCCC will host four **virtual**, multi-day CCN faculty events in June 2025 to develop CCN Course Templates for 47 courses across 18 disciplines. Phase III convening, discipline, and course information can be found on the [ASCCC CCN webpage](#) in the Phase III CCN Implementation section.

ASCCC invites Academic Senate Presidents at all California Community Colleges to nominate up to two (2) faculty members per discipline - or by course as indicated.

The requested nominations are for participation in CCNFWs during the multi-day convenings for disciplines new to CCN, and to fill any potential openings in existing CCNFWs. Please be aware that while we value all nominations, not all nominated faculty may be selected for the final composition of the workgroups.

Convening Date and Time A

June 2, 3, 4, 5
(1pm - 4pm)

Disciplines

Administration of Justice—Melissa Matuszak

* Child Development

* Early Childhood Education – **Amber Lappin**

History

Philosophy—Kevin Maroufkhani

Nomination Notes

* Child Development and Early Childhood Education courses will be addressed by a single CCNFW.

--continued next page

Convening Date and Time B

June 9, 10, 11
(1pm - 4pm)

Disciplines

* Biology (Anatomy & Physiology) –Ryan Joseph and Gregory Russell

* Biology (Microbiology)—Heather Smith

Communication Studies

** English as a Second Language—Miguel Reid and Carla Reible

Political Science—Mark Sellick and Parissa Clark

Nomination Notes

* Two CCNFWs will be formed for Biology with one group addressing Anatomy & Physiology and one group addressing Microbiology. Nominations should be by course for this discipline - two for A & P and two for Microbiology.

** Faculty nominated for this discipline should teach academic reading and writing for multilingual learners.

Convening Date and Time C

June 16, 17, 18
(1pm - 4pm)

Disciplines

Art History

Chicana/o Studies

Kinesiology—Doug Finfrock

Music—Steven Schmidt

--continued next page

Convening Date and Time D

June 23, 24, 25, 26
(1pm - 4pm)

Disciplines

Accounting

* Business

Mathematics—Veasna Chiek and Valerie Merrill

** Psychology

*** Sociology –Michael Chavez and Janet Hill

Nomination Notes

* Faculty nominated for this discipline should include, but not be limited to, those who teach a Business Statistics course as possible.

** Faculty nominated for this discipline should include, but not be limited to, those who teach a Psychology Statistics course as possible.

*** Faculty nominated for this discipline should include, but not be limited to, those who teach a Sociology Statistics course as possible.

--END--