SECURITY MASTER PLAN

For

San José / Evergreen Community College District

Submitted by:

CATALYST Consulting Group, Inc.
2789 Napa Valley Corporate Way, Suite D
Napa, CA 94558

July 27, 2012

SECURITY MASTER PLAN

San Jose/Evergreen Community College District

July 27, 2012

Table of Contents

SECURITY MASTER PLAN

San Jose/Evergreen Community College District

July 27, 2012

1. EXECUTIVE SUMMARY

This Security Master Plan (SMP) has been developed for San Jose/Evergreen Community College District by CATALYST Consulting Group, Inc., a professional consultancy with specific expertise in security planning and design for public institutions and college environments. The SMP is a revised and updated version of the original SMP developed by CATALYST for the District in 2006.

The primary intent of the Security Master Plan is to provide the District with a criteria based system for the selection and implementation of physical and electronic security hardware for new and existing buildings. To accomplish this goal, the Security Master Plan will begin with an explanation of the statistical and anecdotal data CATALYST used to assess the threats faced by District staff, faculty, students, and property. The plan will then provide a detailed evaluation of specific crime statistics data collected for the areas inclusive of and surrounding both the San Jose City College campus and the Evergreen Valley College campus. Next, the plan will provide detailed information collected during numerous site, building, lighting and landscaping surveys conducted on each campus as well as information collected during informal interviews held with various staff and faculty. The data and evaluation gathered from the crime statistics analysis and the surveys will be used to provide a vulnerability/risk analysis for each campus. The vulnerability/risk analysis will in turn be used to then provide detailed recommendations that CATALYST believes will mitigate many of the potential identified threats and thereby provide the District with viable solutions to increase safety and security on the campuses.

Included among the specific recommendations that this plan will address are:

- The need to increase District Police staffing levels to provide an adequate and responsive 7/24 police presence on both campuses.
- Reconfiguration and modernization of the Security Command/Dispatch Center.
- Installation and configuration of a District wide Access Control and Alarm Monitoring System, Digital Video Surveillance System, and Security Communication System.
- Detailed criteria and guidelines for building, parking and site location selection of field electronic security filed devices that function as part of the recommended security systems.

- The addition of Video Surveillance System cameras and equipment to high value/high attractive nuisance targets, i.e. the newly installed solar panel field at Evergreen Valley College.
- Maintenance to existing light fixtures and the addition of new light fixtures at select locations on the campuses.
- Security landscaping guidelines and recommendations.
- Installation and configuration of a District wide Access Control and Alarm Monitoring System, Digital Video Surveillance System, and Security Communication System.
- Detailed criteria and guidelines for building, parking and site location selection of field electronic security filed devices that function as part of the recommended security systems.

2. INTRODUCTION

San Jose/Evergreen Community College District (SJECCD or District) engaged the services of CATALYST Consulting Group, Inc. (CATALYST) to develop a Security Master Plan (SMP) for the District campuses. This report focuses on the security concerns and provides security recommendations for both San Jose City College and Evergreen Valley College.

CATALYST is a Security Consulting firm headquartered in Napa, CA. with over twenty five years of professional experience in security planning, assessment, vulnerability analysis, risk mitigation, systems evaluation, systems design and integration, systems specifications, cost analysis, vendor evaluation, system and vendor selection, construction administration, and system testing. CATALYST has recently performed Security Assessment and Master Planning services for West Valley Mission Community College District, Foothill Community College, Chabot Las Positas Community College District, Santa Rosa Community College District, Dominican University, Saint Mary's College, and University of California - Merced.

The primary intent of the SMP is to provide the District with a set of guidelines and recommendations for the selection, implementation, management and operation of programmatic, procedural, physical, electronic, environmental and behavioral security modifications designed to minimize risk and maximize the protection of the District's employees, students, property and information. It is further the intent of the SMP to define campus standards for the security systems and hardware to be utilized in new and existing buildings. The security systems include the Access Control and Alarm Monitoring System (ACAMS), the Video Surveillance System (VSS), and the Security Communication System (SCS).

The Security Master Plan uses Vulnerability/Risk Analysis as a foundation for developing guidelines and recommendations and incorporates an assessment of current threats faced by District. The Vulnerability/Risk Analysis is further used to define the priorities for a set of risk mitigation recommendations. To develop the Security Assessment, CATALYST has performed numerous site surveys and interviews, analyzed crime index data, reviewed the relevant technologies, and assessed the facilities physical environment with respect to the safety and security of students, staff and property.

To present this information in a clear and cogent manner, CATALYST has divided the SMP into five sections. Each section is intended to provide specific and detailed

information on the Section topic, which serves to further develop information presented in subsequent sections. Section 3, *Sources of Information*, provides background information regarding the sources and methods of acquiring the data necessary to develop the Security Assessment. Section 4, *Crime Statistics and Information Analysis*, presents detailed crime information data useful in providing a benchmark for analysis during the surveys and required to develop the vulnerability and risk assessment. Section 5, *Survey Findings*, includes pertinent information gathered during the Site Surveys, Security Program and Personnel, Electronic Security Systems, Key Control Survey, Lighting and Landscaping Survey, and Interviews with Staff. Section 6, *Vulnerability/Risk Analysis* utilizes the relevant information gathered during the survey process as well as crime statistics analysis to detail the vulnerabilities and risks faced by the District. Section 7, *Recommendations,* includes an examination and evaluation of the existing Security Policy and Procedures as well as recommended changes and enhancements focused on these policies and procedures and mitigation measures to heighten the security of the campuses.

The recommended changes and enhancements included within this document are focused on the District's electronic, programmatic, and physical security programs and are intended to lower the vulnerabilities to the prioritized risks delineated throughout this document. Since the campuses will receive new buildings as well as renovations of existing buildings, these two conditions are treated separately in the recommendations section on Physical Security. For the purpose of the SMP, "Existing Building Renovation" should be taken in reference to security system replacement and/or upgrades and is not intended to imply or be related to Architectural and/or Tennant Improvements to existing buildings. The goal of the recommendation listing is to provide the District with a system to evaluate specific operational and procedural enhancements as well as to delineate specific locations where new security devices will be installed utilizing an objective ranking system.

3. SOURCES OF INFORMATION

To achieve the multi-faceted goals of the Security Master Plan, CATALYST utilized data gathered from three primary sources: crime statistics, site surveys, and interviews. The information collected is utilized throughout this report and is applicable to each of the subsequent sections. This Section details the relevance of the data as well as the processes used to gather this data.

3.1 Crime Statistics

Statistical data representative of crime levels in the areas surrounding the College campuses was collected from various sources for the purpose of providing a benchmark against which the survey information was to be evaluated. Using the Uniform Crime Reporting Index (UCR), published by the Federal Bureau of Investigation, Clery Act Statistics reported by the District and CAP Index reporting, CATALYST extrapolated crime threat probabilities relevant to the campus. The statistical data includes an analysis of local, county and neighborhood crime levels compared to state and national incident statistic averages. This data was used in conjunction with the survey findings and interview data to provide a baseline for the Vulnerability/Risk Analysis.

Uniform Crime Reporting

The Uniform Crime Reporting Program classifies offenses into two groups, Part I and Part II offenses. Each month, contributing agencies submit information on the number of Part I (Crime Index) offenses known to law enforcement. Part 1 offenses are further grouped into two categories, violent crimes (those committed against persons) and non-violent crimes (those committed against property). Violent crimes include criminal homicide, forcible rape, robbery and aggravated assault. Non-violent crimes include burglary, larceny, and motor vehicle theft. These seven crimes and associated population statistics for the reporting agencies jurisdictional area have been the basis of the UCR Crime Index since its inception in 1929. In 1979, data on Arson was added to the list and used to develop the Modified Crime Index. Brief definitions of the Part I offenses are included in Section 4.1.

Clery Act

Clery Act statistics are specific crime statistics data reported to the Federal Government in compliance with the 34 CFR 688.46, “The Jeanne Clery Discloser of Campus Security Policy and Campus Crime Statistics Act” enacted in 1989. The Clery Act requires all college and universities receiving federal financial aid funding keep and disclose crime statistics on Campus and in the surrounding area in an Annual Campus Security Report

issued to the US Department of Education by October 1 each year. As a POST certified agency, the San Jose Evergreen Community College District Police Department reporting requirements required to comply with Clery Act are essentially the same as the reporting requirements to the Federal Bureau of Investigation for the UCR. Therefore, for the purposes of this SMP, review of the Clery Act statistic published by the District is primarily limited to verification that the reported statistics are consistent with those included in the UCR.

CAP Index

Both Clery Act and UCR statistics include population as the only benchmark index in comparing criminal activity in a local jurisdiction to jurisdictional, county and national averages. Because of this CATALYST obtained a report from an independent outside agency that includes socio-economic demographic information as an additional benchmark. This report was generated by CAP Index, Inc., a private company founded in 1988, specializing in loss, risk and crime forecasting, prevention and analysis. CAP Index reports have been accepted in courts for both civil and criminal litigation purposes throughout the country as a reliable statistical tool for crime projections. The crime analysis report is derived from informational databases that contain current socio-economic demographic data and crime statistics (current and past) for the immediate reporting district in which the target facility is located.

CAP Index reports are based on a CRIMECAST score. CRIMECAST scores are derived from an evaluation system designed to accurately identify the risk to personnel and/or property at any location in the United States. The CRIMECAST model is based upon the strong relationship that exists between a neighborhood's "social disorganization" and the amount of crime that is perpetrated there. The CAP Index report includes CRIMECAST scores for each of seven crime types listed in the FBI’s UCR as Part I Offenses, as well as an overall Crimes Against Persons score, an overall Crimes Against Property score, and an overall CAP Index score. The CAP Index score is a weighted average of the homicide, rape and robbery scores. The emphasis is placed on these three (3) crimes because they pose the greatest danger to the public.

CRIMECAST scores indicate a site's risk of crime in comparison to the National, State or County average. The scores are scaled so that a value of 100 is equal to the National, State or County average. Scores over 100 represent above-average predicted crime risks, while scores under 100 indicate below-average risks. Dividing the CAP Index

scores by 100 provides a greater (or lesser) percentage of likelihood of occurrence compared to National, State and County averages.

In addition to the Current Scores tabulated in the CAP Index report, there are historical (Past Scores) and expected future (Projected Scores) tabulations. These figures are valuable in security assessment and planning because they provide added historical evidence and develop predictions for trends in future crime.

Finally, the report includes a Site Map depicting the crime risk surrounding the target location. The Site Map shows CAP Index scores in comparison to the national average for the current time period. The CRIMECAST scoring methodology involves the creation of two circles around the target site: the first circle at a maximum radius of one (1) mile or a population threshold of 25,000 people, and the second circle at a maximum radius of three (3) miles or a population threshold of 100,000 people. Both circles are shown on the Site Map, along with the CRIMECAST scores for each census tract that falls within these circles. The Site Map is included to enhance the data presented in the CRIMECAST assessment.

3.2 Surveys

Key information used in the preparation of the SMP was data collected during the survey process regarding perceived threats and vulnerabilities on each campus. Surveys included:

- An examination of the campus, its buildings, structures, athletics facilities, and solar panel field together with review of the currently implemented risk mitigation measures, which was used to assess the extent of applied physical security methods and their effectiveness.
- A lighting and landscaping survey conducted to evaluate the quality and consistency of each on Campus from a safety and security perspective.
- A review of the safety and security Policies and Procedures.
- Interviews with District and District stakeholders.

The survey process examines the site location, vehicular access to and through the site, parking, the architectural configurations of site buildings and structures, and access to and security of athletic facilities. Where employed, existing electronic physical security systems, chiefly ACAMS, VSS and ECS are evaluated. The methodology employed by

CATALYST in conducting the physical site, building, lighting and landscaping surveys is based on the principles of Timothy Crowe's Crime Prevention Through Environmental Design. The primary focus was on: "Concentric Circles of Protection" and "Natural Surveillance".

> Concentric Circles of Protection is based on varying levels of protection originating at the external area and becoming increasingly more stringent as one proceeds through each level to reach the most critical area (center). Intervention zones are created to provide control locations and/or detection areas. Examples include the building entry points, monitoring of emergency exit only perimeter doors, interior motion detection and/or glass break detection, and interior access control and alarm doors protecting sensitive internal areas.
>
> Natural Surveillance centers on one's ability to view the space around them, maximize visibility, and thus increase one's awareness and reduce the vulnerability for crime. Natural surveillance concepts focus on exterior conditions that effect surveillance, primarily lighting and landscaping, as well as interior areas of surveillance including building access, departmental access and access to sensitive interior areas.[1]

In conjunction with the CPTED methodology, possible constraints to the implementation of physical security measures to the existing site and buildings on the Campuses were examined in detail. While the recommendations for physical security systems are generally broad in nature, the detailed system manufacturers and devices that meet these general requirements should be tailored to provide the desired functionality at the lowest cost to the District. As such, the age of the existing structures as well as the historic and architectural aesthetics of both the original and newer buildings on campus deserve consideration when evaluating and recommending physical systems and devices. Therefore, a significant portion of the site and building surveys were dedicated to the evaluation of the feasibility of installation of various physical security devices.

[1] Timothy Crowe's Crime Prevention Through Environmental Design (CPTED), Second Edition, (Butterworth Heineman, 2000)

3.3 Lighting and Landscaping

One of the principle areas of investigation during the survey process was the evaluation of exterior nighttime lighting levels. In concurrence with the CPTED methodologies, the Illuminating Engineering Society of North America (IESNA) has published the Guideline for Security Lighting for People, Property, and Public Spaces that promote the concept of Natural Surveillance and reinforces the necessity for adequate security lighting. While this guideline has been established by the IESNA, there is no current national standard for protective or security lighting. Formerly there was ANSI A85.1-1956 (R1970), American National Standard for Protective Lighting issued in 1956 and reaffirmed in 1970. This standard has since been withdrawn and no formally adopted standard has been issued. However, the IESNA is the recognized technical authority on illumination and so through its technical committees; it publishes recommended guidelines and practices regarding lighting applications (Security Lighting being one such application), design guides, and technical memoranda. The Society also works with related organizations, such as the American National Standards Institute (ANSI), in the production of jointly published documents and standards. There are other organizations that offer lighting level recommendations as well (the United States Department of Army, Field Manual 3-19-30 and the Architectural Graphics Standards, for example) but their recommendations tend to be organizationally specific and therefore not as universally applicable as the IESNA guidelines. And so until a new ANSI Security Lighting standard is formally adopted, the IESNA design guidelines are the most widely used and recognized reference for Security Lighting in the industry. Included in this guideline are the General Principles for Security Lighting, which are as follows:

- Integration of illumination into the total security system to thereby facilitate the effectiveness of other security devices or procedures.
- Illumination of objects, people, and places to allow observation and identification and thereby physically reduce criminal concealment.
- Illumination to deter criminal acts by increasing fear of detection, identification, and apprehension.
- Lessening the fear of crime by enhancing their perception of security.
- Illumination that allows persons to more easily avoid threats, and to take defensive action when threats are perceived.[2]

[2] IESNA G-1-03 Guideline for Security Lighting for People, Property, and Public Spaces (2003)

In planning security lighting design, there are basic considerations that should be examined. These include an evaluation of the crime statistics in the area, the nature and layout of the site in consideration, the degree of obstruction from landscaping and building configurations, the ambient luminance of the area and the potential impact that additional or reduced lighting will have on the surrounding area and neighborhood. Planning should focus on achieving a balance in these areas while ensuring that the Principles of Security Lighting are maintained. In deciding upon a general plan, specific considerations for luminance should be considered, including:

- *Uniformity:* the evenness of the distribution of light. The higher the level of uniformity the greater one's ability to perceive their surroundings. Uniform light distribution, regardless of intensity, reduces the occurrence of shadows and generally decreases glare, both of which reduce the need for the eye to adjust to varying levels of light.
- *Shadow:* an area that is not illuminated or is only partially illuminated because an interfering object blocks all or some of the radiation emitted from a source. Shadows reduce the effectiveness of security lighting, especially when they are sharply defined, because they reduce perception and decrease uniformity.
- *Glare:* the sensation produced by luminances that are sufficiently greater than the luminance to which the eyes are adapted. While the level of glare varies, if sufficiently high, it can cause annoyance, discomfort and loss of visual performance, all of which generally reduce the effectiveness of security lighting and have a negative impact on uniformity.
- *Color Rendition:* the ability to discern and distinguish color in the surrounding area. Color rendition is an important consideration in security lighting in that the greater the ability to accurately see color, the greater the ability to accurately identify ones surrounding. Key factors that affect the ability to render color include Color Rendering Index, Color Temperature, and Spectral Power Distribution.
- *Color Rendering Index (CRI):* a method of measuring and specifying the color rendering properties of a light source. A

perfect blackbody light source (one having a perfectly even distribution of light across the visible spectrum) has a color rending index of 100. While all light sources have a CRI of less than 100, Standard Incandescent and Tungsten Halogen lamps have CRIs so close to 100 as to be indistinguishable from a perfect blackbody. The higher the CRI the better the color rendering ability of the source. Studies have shown that any white light source with a CRI greater than 50 allows accurate color identification in public spaces at night. Additionally, high pressure sodium lights (yellow), when at higher illuminance levels allow for accurate but less confident color identification.

- *Correct Color Temperature (CCT):* the absolute temperature value (measured in degrees Kelvin) is the temperature that a blackbody must reach to emit a specific color light. Ironically, "warm" light sources (yellow – high pressure sodium and white – warm fluorescents) range in temperature from 1800K to 3200K while "cool" light sources (white - metal halide, white – cool fluorescents, white – LED) range in temperature from 4000K to 7500K.
- *Spectral Power Distribution (SPD):* the power at which a particular light source emits across various wavelengths. A perfect blackbody will emit light of equal power across the visible spectrum. Such a SPD is necessary to produce a CRI of 100. Electric light sources emit radiation with unequal power distributions across the visible spectrum. This inequality in SPD effects the way in which objects appear when illuminated by a specific light source. For example, if a light source is weak in emitting light at the red end of the spectrum, objects illuminated by that light source will appear dull under the source at night.

In addition to the general plan consideration listed above, site and organizationally specific criteria for lighting should be considered as well. These could include architectural, aesthetic, social, economic, maintenance, control, and technological factors. While these considerations are certainly valid and must be included in the final lighting analysis, they are largely beyond the scope and purpose of this report. That said,

the New Buildings Institute, Inc. has published Advanced Lighting Guidelines (2003) that thoroughly reviews and examines these and other lighting considerations and can serve as a valuable tool to assist in general lighting planning and design. This Guideline is extensive and while reiterating many of the CPTED and IESNA recommendations for security lighting, the treatise covers virtually all new construction applications and conditions and could serve as an excellent supplementary reference for the College. A brief review of the technologies covered in depth in the Guidelines that are specific to the College in relation to the security and safety lighting is included below.

In generalized terms, color rendering (CCT, CRI and SPD) have a discernible effect on security lighting in that the higher value of each that a given light source possesses, the greater an individual's ability to discern the correct color and thus, the greater the likelihood to identify the surroundings, thus enhancing natural surveillance. From this point, it is common to make the assumption that lights with relatively high values of each are better in all security applications than lights with lower relative values. In reality, light sources with lower relatively values, in specific applications, often have a better performance in the areas that affect uniformity, particularly glare and shadowing, which deteriorate natural surveillance. From the security perspective, high uniformity with high color rendering is ideal. However, in many applications, a trade off between these two must occur. In these situations, uniformity is generally more critical to perceptions of safety than an acute perception of color rendering. Metal halide lamps (that typically have a CCT 3000-6000K, a CRI of 65-90 and an SPD rendering white light) provide excellent uniformity as well as a high color rendering when in a high mast, high intensity, down cast output application, like parking lots. Contrarily, these same lamps, when used in a low mast, low to medium intensity, post top application, typical of pedestrian walkways and parks, exhibit poor uniformity because of the glare ("hot spots") apparent when attempting to looks past or through the light source. Additionally, objects that are lay outside of the direct light distribution pattern of a given lamp tend to appear in shadow because less of the generated light is reflected of surrounding objects, which further reduces uniformity. In these applications, high pressure sodium lamps (that typically have a CCT of 1800-2200K, a CRI of 22-35 and an SPD rendering yellow light) are selected because uniformity is maintained even though color rendering ability is reduced. The glare produced by the yellow light emitted by high pressure sodium lamps is low in comparison to metal halide. Also, since the emitted light has a distinctly narrow bandwidth (which equates to a narrow SPD) the quantity of light reflected by the surrounding is greater than with metal halide, which has a tendency to reduce the occurrence of shadows, also increasing uniformity. Finally, one of the chief factors that

reduce the uniformity of light distribution is a combination of different lamp technologies in the same field of view. Regardless of lamp technology, consistency in application is critical.

3.4 Interviews

Informal interviews with various District and College personnel were included in the survey process to provide insight into whether the current physical security mitigation measures were in line with the personnel's perceived sense of vulnerability. The interviews provided key insights from staff with specific regard to perceptions of safety and security of personnel, students and property within the facilities on campus, effectiveness of existing security systems and procedures, departmental perceptions of vulnerabilities, perceptions of Police staffing levels, and perceptions of general security awareness. The information gleaned from the interviews is particularly important because, in addition to providing the aforementioned perceptions, they also provide a point of reference for balancing the effectiveness of current educational culture with increasing vulnerabilities experienced as a result of campus growth.

In addition to these informal interviews, detailed discussions were conducted with individuals in the District Police Department. The purpose of these interviews was to gather programmatic, operational, procedural, and system specific security information on the District as a whole as opposed campus and departmentally specific data.

The information gathered from these various sources is included within the remainder of this assessment, specifically in the categories of Survey Findings, Vulnerability/Risk Analysis, and Recommendations. Within these sections are to be found details of the identified threats and vulnerabilities at each campus, an examination of existing physical and procedural security measures and the recommendations that CATALYST believes will enhance the safety and security of the San Jose/Evergreen Community College District's students, staff, and property.

4. CRIME STATISTICS INFORMATION AND ANALYSIS

"No security plan or program can be effective unless it is based upon a clear understanding of the actual risks it is designed to control."[3] In assessing vulnerability to crime for the District, CATALYST gathered statistical historic crime data from the Uniform Crime Report – 2005 published by the FBI. In addition to this historical data, CATALYST obtained a crime statistic and analysis report from CAP Index, Inc.

4.1 FBI Uniform Crime Report (UCR)

The Uniform Crime Reporting Program classifies offenses into two groups, Part I and Part II offenses. Each month, contributing agencies submit information on the number of Part I (Crime Index) offenses known to law enforcement. Part 1 offenses are grouped into two categories, violent crimes and non-violent crimes. Violent crimes include criminal homicide, forcible rape, robbery and aggravated assault. Non-violent crimes include burglary, larceny, and motor vehicle theft. These seven crimes and associated population statistics for the reporting agencies jurisdictional area have been the basis of the UCR Crime Index since its inception in 1929. In 1979, data on Arson was added to the list and used to develop the Modified Crime Index. Brief definitions of the Part I offenses are included below.[4]

- Criminal Homicide: a) Murder and non-negligent manslaughter: The willful killing of one human being by another. Deaths caused by negligence, attempts to kill, assaults to kill, suicides, and accidental deaths are excluded. b.) Manslaughter by negligence: the killing of another person though gross negligence. Traffic fatalities are excluded. [3]

- Forcible Rape: The carnal knowledge of a female forcibly and against her will. Rapes by force and attempts or assaults to rape regardless of the age of the victim are included. Statutory offenses are excluded. [3]

- Robbery: The taking or attempting to take anything of value from the care, custody, or control of a person or persons by force or threat of force or violence and/or by putting the victim in fear. [3]

[3] Walsh, CPP, Timothy J., Protection of Assets Manual, The Merritt Company; 1991, Vol. 1 p.2-1
[4] Federal Bureau of Investigation, Uniform Crime Report, Appendix II – Offenses in Uniform Crime Reporting.

- Aggravated Assault: An unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. This type of assault is usually accompanied by the use of a weapon or by means likely to produce death or great bodily harm. Simple assaults are excluded.[3]
- Burglary: The unlawful entry of a structure to commit a felony or a theft. Attempted forcible entry is included.[4]

- Larceny: The unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another. Examples include thefts of bicycles or automobile accessories, shoplifting, pocket picking, or stealing of any property or article, which is not taken by force or by fraud. Attempted larcenies are included. Embezzlement, forgery, worthless checks, etc. are excluded.[5]

- Motor Vehicle Theft: The theft or attempted theft of a motor vehicle. A motor vehicle is self-propelled and runs on the surface not on rails. Motorboats, construction equipment, airplanes, and farming equipment are specifically excluded.[4]

- Arson: Any willful or malicious burning or attempt to burn, with or without intent to defraud, a dwelling house, public building, motor vehicle, aircraft, personal property of another, etc.[4]

Part 2 offenses, which include Vandalism, Disturbances, Fraud and Forgery, Trespassing, Traffic and Parking Violations, Threats and Restraining Order Violations, are lesser magnitude crimes and are not tracked in the UCR. However, the risk associated with these types of offenses will be included in the Vulnerability/Risk Analysis section of this report.

The following table includes data from the UCR for 2004 through 2010 for the San Jose/Evergreen College District. The UCR does not divide the statistics per campus because the District Police are a single reporting agency. At the time of writing, data from 2011 is not yet available from the FBI.

[5] Federal Bureau of Investigation, Uniform Crime Report, Appendix II – Offenses in Uniform Crime Reporting.

Data was included from 2004 onward because the data examined in the original SMP included years 2004 and 2005. By including these years in this version of the SMP, along with the intervening years, a greater understanding from trending analysis can be gleaned.

	Population	Violent Crime	Property Crime	Murder	Forcible Rape	Robbery	Aggravated Assault	Burglary	Larceny	Motor Vehicle Theft	Arson
2004	19,943	0	125	0	0	0	0	16	103	6	2
2005	19,422	1	76	0	0	0	1	12	61	3	0
2006	18,772	4	76	0	0	2	2	16	60	0	0
2007	18,164	0	79	0	0	0	0	10	63	6	2
2008	18,512	0	60	0	0	0	0	4	53	3	0
2009	22,826	0	81	0	0	0	0	3	69	9	0
2010	23,550	3	53	0	1	1	1	2	50	1	0

The following table includes data from the UCR for 2004 and 2010 for the City of San Jose. This information is included for the evaluation of trends between crime on campus and crime in the neighborhoods surrounding the campuses.

	Population	Violent Crime	Property Crime	Murder	Forcible Rape	Robbery	Aggravated Assault	Burglary	Larceny	Motor Vehicle Theft	Arson
2004	908,712	3,379	22,298	24	256	785	2,314	3,616	14,165	4,517	248
2005	910,528	3,492	22,930	26	263	884	2,319	4,049	13,374	5,507	388
2006	920,548	3,561	24,240	29	217	1,030	2,285	4,423	12,678	7,139	437
2007	934,553	3,759	24,062	33	217	1,068	2,441	4,449	13,200	6,413	339
2008	945,197	3,643	22,298	31	220	1,124	2,268	3,457	13,612	5,229	288
2009	954,009	3,439	22,755	28	258	1,025	2,128	3,741	13,635	5,379	243
2010	970,252	3,215	22,801	20	253	976	1,966	3,940	12,730	5,411	181

By examining these UCR data, it is evident that, while there was an apparent spike in crime on the campuses in 2004, levels dropped significantly in 2005 and have remained statistically consistent from 2005 through 2010.

The spike in crime was not apparent in the UCR data for the City of San Jose in 2004. But the overall crime rates within the City data are statistically consistent similar to the rates on the campuses. Further trend comparison information is included in Section 4.3 – Concluding Analysis.

4.2 CAP Index Report

CAP Index reports are based on a CRIMECAST score. CRIMECAST scores are derived from an evaluation system designed to accurately identify the risk to personnel and/or property at any location in the United States. The CRIMECAST model is based upon the strong relationship that exists between a neighborhood's "social disorganization" and the amount of crime that is perpetrated there. The CAP Index report includes CRIMECAST scores for each of seven crime types listed in the FBI's UCR as Part I Offenses, as well as an overall Crimes Against Persons score, an overall Crimes Against Property score, and an overall "CAP Index" score. The CAP Index score is a weighted average of the homicide, rape and robbery scores. The emphasis is placed on these three (3) crimes because they pose the greatest danger to students, staff and the general public. CRIMECAST scores indicate a site's risk of crime in comparison to the National, State or County average. The scores are scaled so that a value of 100 is equal to the National, State or County average. Scores over 100 represent above-average predicted crime risks, while scores under 100 indicate below-average risks. Dividing the CAP Index scores by 100 provides a greater (or lesser) percentage of likelihood of occurrence compared National, State and County averages.

The "Current Scores" for 2012 are based on UCR data from 2010. In addition to the "Current Scores" tabulated in the CAP Index report, there are historical ("Past Scores") and expected future ("Projected Scores") tabulations. These figures are valuable in security assessment and planning because they provide added historical evidence and develop predictions for trends in future crime.

Specific CRIMECAST Details and Statistical Mapping

Current Scores – San Jose City College

Current Scores (2012)	**National Scores**	**State Scores**	**County Scores**
CAP Index	142	112	179
Homicide	101	76	144
Rape	93	94	176
Robbery	167	126	189

Aggravated Assault	138	123	183
Crimes Against Persons	135	115	178
Burglary	111	101	210
Larceny	118	148	148
Motor Vehicle Theft	241	134	207
Crimes Against Property	126	130	163

Past Scores (2000) – San Jose City College

Past Scores (2000)	**National Scores**	**State Scores**	**County Scores**
CAP Index	138	114	209
Homicide	95	70	121
Rape	179	176	287
Robbery	152	120	219
Aggravated Assault	192	163	236
Crimes Against Persons	171	144	229
Burglary	185	159	313
Larceny	142	182	212
Motor Vehicle Theft	235	122	225
Crimes Against Property	151	153	226

Future Scores (2017) – San Jose City College

Projected Scores (2017)	**National Scores**	**State Scores**	**County Scores**
CAP Index	144	112	171
Homicide	104	77	131
Rape	83	83	164
Robbery	171	127	182
Aggravated Assault	124	107	174
Crimes Against Persons	128	106	170
Burglary	107	95	196
Larceny	106	127	137
Motor Vehicle Theft	204	113	174
Crimes Against Property	114	113	150

In addition to the detailed CRIMECAST score information, the report includes a Site Map depicting the crime risk surrounding the target location. The Site Map shows "CAP

Index" scores in comparison to the national average for the current time period. The CRIMECAST scoring methodology involves the creation of two circles around the target site: the first circle at a maximum radius of one (1) mile or a population threshold of 25,000 people, and the second circle at a maximum radius of three (3) miles or a population threshold of 100,000 people. Both circles are shown on the Site Map, along with the CRIMECAST scores for each census tract that falls within these circles. The Site Map is included to enhance the interpretation of a CRIMECAST assessment. (See following page)

Site Map – San Jose City College

Specific CRIMECAST Details and Statistical Mapping

Current Scores – Evergreen Valley College

Current Scores (2012)	National Scores	State Scores	County Scores
CAP Index	59	47	74
Homicide	77	58	109
Rape	40	40	76
Robbery	71	54	80
Aggravated Assault	99	88	131
Crimes Against Persons	80	68	105
Burglary	60	55	113
Larceny	48	60	60
Motor Vehicle Theft	93	52	80
Crimes Against Property	50	51	65

Past Scores (2000) – Evergreen Valley College

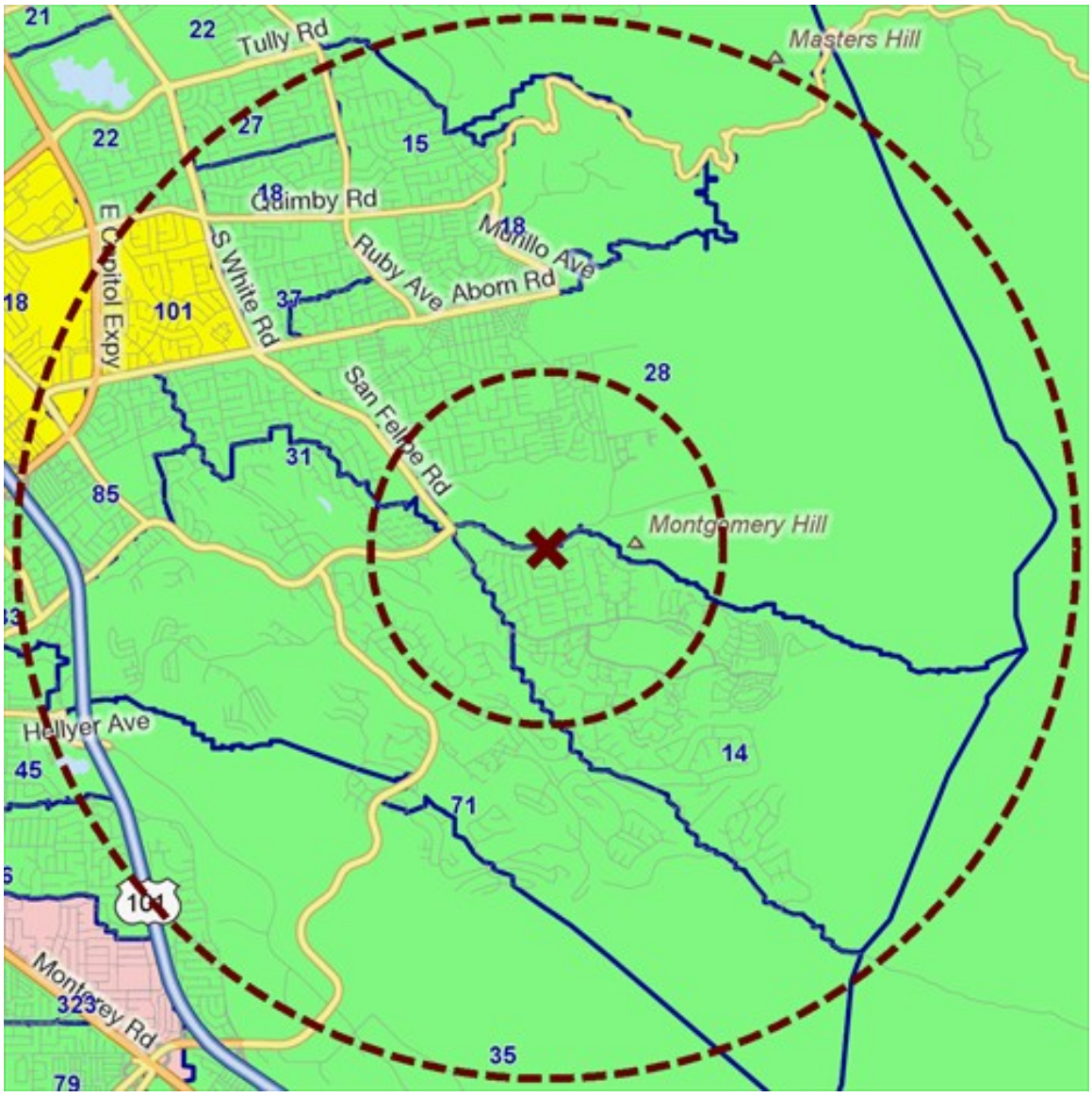
Past Scores (2000)	National Scores	State Scores	County Scores
CAP Index	57	47	86
Homicide	95	70	121
Rape	68	67	109
Robbery	58	46	84
Aggravated Assault	106	90	130
Crimes Against Persons	85	72	114
Burglary	59	51	100
Larceny	36	46	54
Motor Vehicle Theft	112	58	107
Crimes Against Property	47	48	70

Future Scores (2017) – Evergreen Valley College

Projected Scores (2017)	National Scores	State Scores	County Scores
CAP Index	59	46	70
Homicide	93	69	117
Rape	36	36	71
Robbery	71	53	76
Aggravated Assault	86	74	121

Crimes Against Persons	72	60	96
Burglary	65	58	119
Larceny	51	61	66
Motor Vehicle Theft	88	49	75
Crimes Against Property	53	53	70

Site Map –Evergreen Valley College



4.3 Analysis

When analyzing statistical crime information, it is useful to look at percentage increase (decrease) as well as the averaged scores. These figures provide insight into trends as well as target specific types of crime that are problematic within a given area. It is clear that Property Crimes, particularly Burglary and Larceny, pose the greatest risk on the San Jose City College and Evergreen Valley College campuses. As assessing the CAP Index Past and Future projected crime scores, it is clearly apparent that, while slight variations may be occur from year to year, the overall average scores have been and are expected to be consistent or slightly increasing in coming years. As such, mitigation efforts aimed at reducing these types of crime on the campuses in the short-term will likely provide continuing mitigating benefits over the long-term.

Additionally, as mentioned at the end of Section 4.1 – FBI Uniform Crime Report (UCR), trends in criminal activity in the areas surrounding the campuses does not equate to increased crime on campus. Analysis of crime on college campuses in the United States indicate that the predominant threat comes from perpetrators of victimization crimes, whether against property or persons. In 1999, APBnews.com released a study that analyzed some key presumptions about college campus crime and its interrelationship to the surrounding community. Representative of nearly 1,500 college campuses, and using data collected from CAP Index, Inc, the Bureau of Justice, the FBI Uniform Crime Reports, and supplemental reports from various police departments, the study is founded on two concepts: 1) that campus personnel use the surrounding areas and are therefore at risk of victimization equivalent to crime in those areas, and 2) that criminals from the surrounding area traveled onto campus to locate victims. The data presented raises the question whether the community setting has an effect on the level of crime on campus, and if the sources of campus crime are from the neighboring community. Certain studies on campus crime[6] imply that we can use risk factors for a larger area to determine the risk of a smaller community within this larger community. While this seems intuitive and is often presented in the media as a likely cause for campus crime, further case studies have proven that these assumptions do not accurately represent the true nature or source of campus crime and in general are misleading. The most comprehensive of the campus crime case studies that followed[7] found that in general, community crime rates and characteristics had little effect on campus crime. In fact, the characteristics of the

[6] Pearson, F.S. and J. Toby (1991). "Fear of School-Related Predatory Crime." *Sociology and Social Research.*
[7] Lizotte, A.J. and A. Fernandez (1995) *Trends and Correlates of Campus Crime: A General Report.*

campus had a stronger and more uniform effect on campus crime rates than the surrounding community; indicating that safety on the campus proper is where emphasis is most needed. The threats already present on campus accounted for most of the source of crimes, with the study finding that over 80% of the reported campus crimes were perpetrated by other students. The only exceptions to this finding were robbery and auto theft, where crime rates in the neighboring community did affect the statistical occurrences and frequency of these events on campus. It was concluded that these two categories of crime were committed by criminals who targeted both students and community residents alike, and were the two crimes that perpetrators were willing to travel the farthest to commit. In examining the UCR and CAP Index data provided above, it is clear that criminal activity on the San Jose City College and Evergreen Valley College campuses correlate to these national statistical data.

Finally, while the area surrounding San Jose City College has considerably higher crime rates than the area surrounding Evergreen Valley College, crimes committed on each campus are historically approximately equal in number. This fact is particularly noteworthy for two reasons. Firstly, it indicates that recommended security mitigation measures are, for the most part, equally important on both campuses and can be equally applied to both campuses. Secondly, it is presumable that the greater vigilance and security awareness is exhibited by students and staff on the San Jose City College campus simply through recognition of the security risks inherent with the neighborhood in which the campus is located.

5. SURVEY FINDINGS

5.1 Surveys

Utilizing the CPTED methodological approach described in Section 3, the survey process examined the District's security program including: Police personnel roles and responsibilities; campus locations and vehicular access to and through the campuses; parking; existing electronic physical security systems; security related building architectural configurations; and lighting and landscaping. General risks noted for these areas are discussed within the text that follows and will be further addressed in the Vulnerability/Risk Analysis section. Specific risks are included at the end of each applicable subsection and will likewise be addressed specifically in the Vulnerability/Risk Analysis and Recommendations sections where their potentiality and critically will be equated and mitigation measures will be recommended respectively.

5.2 Security Program and Personnel

Campus Police Roles and Responsibilities

Feeling safe on campus affects the overall quality of education and is interrelated to student recruitment, retention, and ultimately the financial viability of the institution. Campus Police staff generally exhibits the evolution of campus security from earlier roles of primarily property protection to the more current roles of professional policing with an effective humanist orientation. In the campus environment, once the crime has been committed, little can be done in the short-term to remedy the fear and anxiety caused as a result of that crime. Therefore, different from the traditional policing approach of criminal apprehension, the Campus Police focus on crime prevention through community policing and personal relationships on campus.

Security on the San Jose City College and Evergreen Valley College campuses rests within the purview of the District Police. The District Police Department maintains an office on the San Jose City campus that is open between the hours of 7:00 a.m. and 3:00 p.m. and an office on the Evergreen Valley campus that is open between the hours of 7:00 a.m. and 11:00 p.m. The Evergreen Valley campus office additionally serves as the central police dispatch location for the District. At least one officer is on duty at each campus between the hours of 7:00 a.m. and 3:00 p.m. After 3:00 p.m., one officer is assigned to patrol and respond to incidents on both of the campuses until 11:00 p.m.. After 11:00 p.m., District Police do not have a presence on either campus and San Jose Police are relied upon to respond to incidents reported on campus.

It is safe to say that most departments could provide better service with a larger staff, and this is especially true with regard to Campus Police. Currently, the Department is under staffed and tasked with responsibilities that clearly fall outside of the normal scope of responsibilities for Campus Police. As mentioned, there is no police presence on either campus between 11:00 p.m. and 7:00 a.m. and only one sworn officer responsible for policing both campuses between 3:00 p.m. and 11:00 p.m. Additionally, the fact that the area surrounding the San Jose City College campus has roughly twice the crime rate per capita logically indicates that the Police Department office on this campus should not be closed daily at 3:00 p.m. but rather should be open at least until the campus closes.

Additionally, Police Dispatch is tasked with communicating and coordinating non-police related business (facilities, maintenance, and operations related issues) with the appropriate College personnel during business hours. Such communication and coordination responsibilities detracts from the police related dispatch responsibilities and has the distinct potential of delaying timely response to legitimate security issues and/or emergency situations.

Finally, Police Officers are tasked with responsibilities that are not typically within the purview of the Police Department. For example, the collection of receipts from parking permit machines and bank deposit of these receipts. While the collection of receipts from parking permit machines is justifiably a responsibility of Campus Police, bank deposit of such receipts is not. Bank deposits not only require officers to leave campus, thereby jeopardizing their ability to effectively respond to on campus situations, they also represent a potential liability to an officer that must respond to a legitimate police while in transit with said receipts.

It is therefore the opinion of CATALYST that Police understaffing, as well as the lack of effective delineation of Police Department responsibilities represent the greatest deficiencies in safety and security for the District and thereby the greatest area of potential risk found within the scope of this project. As such, the highest priority recommendation, included in Section 7 – Recommendations, is for increased Police staffing and a firm definition of Police roles and responsibilities.

San Jose City College:

The San Jose City College campus is bounded by Moorpark Avenue to the North, Leigh Avenue to the East, Rexford Way and Kingman Avenue to the South, and South Bascom Avenue to the West. Interstate 280 is directly North of Moorpark Avenue, residential

neighborhoods surrounding the campus on the on the Eastern and Southern Boarders and business boarder the campus on the Western boarder. The neighborhood to the South, primarily West of Sherman Oaks Drive, as well as the businesses located between South Bascom Avenue and Laswell Avenue on the western edge of campus have historically presented the majority of the Class 2 criminal offenses (vandalism, trespassing, harassment, etc.) to the campus. The remaining businesses and residential neighborhood communities do not present a historically significant level of crime on the campus. However, it should be noted that crime demographics presented in Section 4.2 – Cap Index Report, should be considered when evaluating potential crime threats form the neighboring communities.

Vehicular and pedestrian traffic to the campus is unrestricted. Access to surface parking lots and the Parking Garage are open from the perimeter streets and parking control is accomplished through the utilization of parking permit machines located in each lot as well as on each floor of the Parking Garage. There are some roads that transit the campus. Access to the roads that are solely used for maintenance and police patrols are, for the most part, controlled through parking arm gates. Access to roads that lead to internal campus staff parking areas are not controlled, in particular, the access road running east and west between the Student Center, Gymnasiums, and Pool and the athletic fields. Of principal concern, noted during the survey and expressed in many of the informal interviews, is the portion of this road that passes the Student Center directly adjacent to the exterior cafeteria dining area. As a result, the introduction of physical parking controls to these areas is included in Section 7 – Recommendations.

During the survey of the surface parking lots and the Parking Garage, the locations of Emergency Call Boxes were evaluated. The Parking Garage is well equipped with four call boxes, equipped with blue location lights, on each floor. These call boxes are strategically placed near the parking permit machines. Surface lots are not equipped with Emergency Call Boxes. Calls that originate from the Emergency Call Boxes are routed to Police Dispatch during the hours that Dispatch is staffed. After-hours, calls are routed to 911. There were some problematic items noted. These include the lack of “equivalent” placement of the call boxes in all lots and contradictory public notice of the use and availability of response. These items are referenced and specific recommendations to mitigate potential risks are included in Section 7 – Recommendations.

Evergreen Valley College

The Evergreen Valley College campus is bounded by Yerba Buena Road to the South and East, San Felipe Road on the West, and Paseo De Arboles and Falls Creek Drive on the North. The northern portion of the campus includes a large undeveloped open area between the campus proper and Falls Creek and Yerba Buena Roads. Residential neighborhoods occupy the areas North and East of this open area. Evergreen Park lies south of the southern portion of Yerba Buena Road and residential neighborhoods occupy the majority of the area further south. Light commercial and retails shops boarder the campus at the Southwest corner of the property along San Felipe Road. With the exception of the Southwest corner of the campus, the Evergreen Valley College site location has little or no direct vehicular or pedestrian access from areas other than the road ways that lead into and through campus. As such, there has not been the same historical occurrence of Class 2 criminal activity spreading onto campus as was witnessed at San Jose City College.

While access to the campus is fairly well limited to the roadways leading into the campus, vehicular and pedestrian traffic to the campus is unrestricted. Access to surface parking lots is open from these roadways and parking control is accomplished through the utilization of parking permit machines located in each lot. There are also a number of roads that transit through the campus. These roads are used for maintenance, police patrols, deliveries, and some staff and disabled parking are. Access to these roads is not controlled, in particular, the access road running east and west that is just north of Gullo Student Center and Physical Education. This roadway is of principal concern, noted during the survey and expressed in many of the informal interviews, because of the extent to which it bifurcates the campus. Since access to this road must remain open for deliveries and handicap parking, the introduction of physical parking controls is included in Section 7 – Recommendations to limit the number and frequency of vehicles upon this road.

Similar to the surface parking lots at the San Jose City College campus, the surface lots at the Evergreen College campus are not equipped with Emergency Call Boxes. However, there are a scattered number of call boxes located throughout the campus. Calls that originate from the Emergency Call Boxes are routed to Police Dispatch during the hours that Dispatch is staffed. After-hours, calls are routed to 911. There were some problematic items noted. The primary item is in reference to contradictory public notice of the use and availability of response. Specific mitigations recommendations are included Section 7 – Recommendations.

Existing Access Control and Alarm Systems

During the surveys, time was devoted to examination and evaluation of the existing electronic card access control and alarm systems.

In general, buildings on both the campuses are of two architectural configurations. The first, which includes the majority of the older building as well some of the newer buildings, is the traditional classroom configuration where each classroom has at least one door leading to the exterior. The second, that includes the majority of the newer buildings, is the "corporate" configuration where primary ingress and egress is thorough a limited number of exterior doors with interior rooms only accessible from within the structure. These two architectural configurations present particular challenges when formulating a coherent plan for the implementation of electronic security systems. This will be further considered and elaborated upon within Section 7 – Recommendations.

Electronic security at both campuses is primarily accomplished through individual building/classroom alarm panels. Field devices attached to these alarm panels include alarm contacts on perimeter doors and, in some cases, interior infra-red motion detectors. The installed alarm contacts provide alarm input notification to the alarm panel when a perimeter door is opened while the alarm panel is active. Motion detectors provide alarm notification to the alarm panel when motion is detected within the internal coverage area when the alarm panel is active. The alarm panels are activated and deactivated via standard pin coded alarm keypads located adjacent to the primary entrance location. When active, the alarm panels transmit received alarm information to a third party central monitoring station that in turn notifies District Police of the alarm event. If an alarm is received during normal Dispatch hours, the third party central station monitoring company notifies Police Dispatch directly. If the alarm is received after normal, the third party central station monitoring company calls an alarm pager that is assigned to one of the off-duty District Police Officers who then responds. While this topological configuration works, the delay in response time, especially during off-hours, severely hampers the ability to provide effective police response to an alarm event. Additionally, each of the alarm panels requires a separate monitoring contract with the third party central station monitoring company. Exact financial figures for the aggregate alarm monitoring contracts was not obtained during the surveys but with two campuses the size of San Jose City College and Evergreen Valley College, the cost is typically $10,000 to $20,000 annually. In addition, after-hours alarm response has an associated cost reflected in overtime pay for the required officer response. These two cost figures are mentioned because they should be weighed when considering the recommendation

of adding additional Police Officers to provide 7/24 presence on the campuses. This will be further elucidated in Section 7 – Recommendations.

In addition to the individual building/classroom alarm panels, newer buildings on the San Jose City College campus are also configured for access control. This application is used solely for entrance control as no alarm related information is connected to nor reported by the access control equipment. The entrance control function is accomplished through the utilization of electronic proximity card readers and electronic locking devices on the associated doors. The primary benefit of the system, as installed on the campus, is to limit the number of issued mechanical keys, relying on issued proximity cards instead. With this system, issued access control cards can be added and removed from the system, thereby obviating the need to mechanically re-key doors if critical keys are lost, stolen or not returned by personnel leaving employment with the College. The card access system in use at the San Jose City College is Win-Pac Pro, by GE/Northern Computers. Even though not currently configured as such, this system is capable of providing alarm information as well as access control. Further information on the benefits of integrated Access Control and Alarm Monitoring Systems is included in Section 7 – Recommendations.

Solar Panel Field

In addition to the new and existing buildings on campus, a new solar panel field has recently been installed at Evergreen Valley College. The solar panel field is large, easily accessible, and represents a substantial District investment. There is currently no electronic security devices or systems installed to mitigate threats against the solar panel field and common CPTED environmental protection strategies are difficult to employ to provide adequate protection. Risks specifically associated with the solar field are numerated in Section 6 – Vulnerability/Risk Analysis and specific mitigation recommendations are included in Section 7 – Recommendations.

Sensitive Internal Areas

Areas within buildings on campus often house information and property that require a higher level of physical and procedural security than can be effectively managed by simply securing the building perimeter. Whether personal information, financial records and data, computer and electronics, specialized equipment, laboratory equipment and machinery, applying the CPTED approach to sensitive internal areas works equally as well as when applied to the building perimeter and site. Electronic alarm and access control systems are often the first line of defense in protecting sensitive internal areas. In

addition to the electronic alarm and access systems, internal areas often rely on Video Surveillance System (VSS) Cameras to provide deterrence, monitoring capability, and recorded video for investigative purposes. While exterior VSS cameras are not currently utilized on the campuses, interior cameras are used in some of these sensitive internal areas.

Many of the individual classrooms, laboratories, and specialty areas on both campuses currently utilize electronic alarm systems to provide an additional internal layer of security for the protection of high value and attractive nuisance materials as well as items that are of lower values but are easily stolen. Some of these areas, particularly campus Bookstores and Student Centers are equipped with older technology Closed Circuit Television cameras. However, it was surprising to find that only the cameras in the Bookstore on the San Jose City College Campus were being monitored and recorded. Cameras in the Evergreen Valley College book store and Gullo Student Center are not functioning and are not connected to monitoring or recording equipment. While the visibility of cameras provides mitigating benefits, the lack of recording renders them worthless once a crime has been committed. As such, VSS camera and recording equipment recommendations are included in Section 7 – Recommendations. Sensitive internal areas that should be considered for VSS camera coverage in additions to electronic alarm monitoring systems include: Libraries, Bookstores, Computer Centers, Athletic Equipment Rooms, Laboratory equipment, chemical and specimens storage areas, the Observatory, the Auto Shop, Weight Rooms, Machine Shops, and the solar panel field.

5.3 Lighting and Landscaping

General Security Lighting Considerations

Factors, which affect Security Lighting, include, but are not limited to the following:

- Crime status of the area
- Nature of the site
- Degree of obstruction: Potential obstruction of light due to landscape design and building configurations.
- Ambient brightness of the surrounding area

Recommended Average Luminance Values for Security Lighting: The following Security Lighting levels are based on the IESNA Lighting Handbook, 9th Edition (2000). For purposes of this document, only horizontal luminance values are listed, other values such as vertical luminance and determination of light characteristics, i.e., color appearance,

glare, shadows, etc., will be interpreted and coordinated with the Campus. For purposes of this document and IESNA luminance values, the Campus was considered a “Public Spaces” because it is an open campus to which there is unrestricted public access. While luminance can be measured in lux (lx) and in footcandles (fc), during the surveys all luminance values were taken in footcandles and all values in this report are presented in footcandles.

IESNA – Recommended Lighting Levels			
		Footcandle (fc)	See Note 1
Large Open Areas:		0.5 to 2	See Note 2
Building Entrances:			
Active		5	
Inactive (normally locked)		3	
Parking Lots		1.0 to 5	See Note 3
Covered Parking Facilities		6	
Parks, Plazas, and Pedestrian Malls		5	
Sidewalks and Footpaths, and		0.6	
Grounds Around Open Parking Lots		0.6	
Trails and Walkways		0.6	
Areas Around Open Parking Lots		0.6	

Notes:

1. A footcandle is a unit used for measuring the amount of illumination on a surface. The amount of usable light from any given source is partially determined by the source’s angle of incidence and the distance to the illuminated surface.
2. The greater the brightness of the surrounding area, the higher the illuminance required to balance the brightness in the space.
3. Below 10 lx (1.0 fc), perceptions of personal safety deteriorate rapidly.

While the IESNA guidelines and recommendations for security lighting have been accepted as standards in lighting design and evaluation, the following is a listing of other standards, not developed solely for security requirements, which are often used for reference and comparison.

Department of Army, Field Manual 3-19-30			
		Foot-candle (fc)	

Outer Perimeter:		0.2	
Restricted Area Perimeter:		0.4	
Vehicular Entrances		1.0	
Pedestrian Entrances		2.0	
Sensitive Inner Areas		0.2	
Sensitive Inner Structure		1.0	
Open Yards		2.0	
Decks and Open Piers		1.0	
Grounds Around Open Parking Lots		0.6	
Trails and Walkways		0.6	
Areas Around Open Parking Lots		0.6	

Architectural Graphics Standards– Recommended Lighting Levels			
		Foot-candle (fc)	
Sidewalks		.02 to .09	
Pedestrian Walkways		.05 to 2.0	
Major Road & Expressway		1.0 to 2.0	
Collector Road		.06 to 1.2	
Parking Lots		1.0 to 5	
Local road		.04 to .09	
Alleys		.02 to .06	
Parking Lots		1.0 to 2.0	
Building Entrances		5.0	
General Grounds		1.0	

During the lighting and landscaping survey, lighting levels were measured using an EXTECH Instruments, model 407026 light meter. All readings were taken in foot-candles and were adjusted based on the lighting source (tungsten, fluorescent, sodium, or mercury). The survey of the San Jose City College campus was conducted between 11:30 p.m. and 1:00 a.m. The survey of the Evergreen Valley College campus was conducted between 9:00 p.m. and 11:00 p.m. The surveys covered exterior areas of each campus, including building perimeters, building entrances, pedestrian walkways, open areas, and parking lots. The information presented in this assessment includes Security Lighting Standards and information, general security landscaping standards in relation to campus lighting, and light level readings in areas that were below the standards as measured during the survey.

Utilizing the previously referenced IESNA guidelines, the following is a listing of the lighting levels measured in areas that were found to be below the recommended levels. Within the following table, where a range of values is indicated, the range includes the lowest measured reading and the highest average reading. Where building entrances are noted, the measurements include readings at the entranceway as well as along the walkway or approach to the entrance. The readings include those that were found to be poor to marginal (poor = significantly lower than the standard, marginal = close to but lower than the standard).

San Jose City College Campus			
Building/Area	Location	Foot-candle (fc)	Rating
Student Center	Northeast Entry	0.3 to 5	Marginal
Drama and Speech	Northeast corner walkway	0	Poor
	North sidewalk boarding Moorpark Ave.	0	Poor
	Northwest corner walkway	0	Poor
New Science Building	East walkway and open area	0 to .2	Poor
	North parking lot	0 to 0.7	Poor
College Union	Staff Parking	0.3 to 6.0	Poor to Good
	Laswell Avenue West of Staff Parking	0 to 0.1	Poor
100, 200, 300 Wings	West Student Parking	0.1 to 6	Poor to Good
	Laswell Avenue West of Student Parking	0 to 0.1	Poor
	South Student Parking	0.1 to 6	Poor to Good
	Student Parking South of 100 Wing	0	Poor
	Staff Parking East of 100 Wing	0 to 7	Poor to Good
	Drive between 100 and 200	0 to 1.6	Poor
	Drive between 200 and 300	0 to 1.6	Poor

Child Development	East sidewalk (along Mansfield Dr.)	0 to 0.1	Poor
	North Parking Lot	0.2 to 2	Poor to Marginal
Central Utilities Plant	North Alley	0	Poor
Auxiliary Gym	North walkway	0 to 0.2	Poor
	Quad North of walkway	0 to 0.1	Poor

Evergreen Valley College Campus			
Building/Area	Location	Foot-candle (fc)	Rating
Child Development Center	South sidewalk	0	Poor
Parking Lot 8	East Side – near Yerba Buena Road	0 to 0.3	Poor
Parking Lot 7	Entire Lot	0 to 0.6	Poor
Parking Lot 6	North and East sides	0 to 0.4	Poor
Acacia	Auto Shop Vehicle Yard	0 to 0.2	Poor
	Auto Tech Yard	0.2 to 0.8	Poor to Marginal
Physical Education	Basketball Courts South of Building	0 to 0.3	Poor
	Access Road North Side of Building	0 to 0.5	Poor to Marginal
Cedro Portables	All walkways	0 to 0.5	Poor to Marginal

*Note – Lighting levels on the access road and walkway to Montgomery Hill Observatory, as well as the Observatory proper were below IESNA standards but are deemed adequate with consideration of the buildings function.

Recommendations for improving and or rectifying the problematic areas noted above are included in Section 7 – Recommendations.

Landscaping:

When evaluating security lighting, the nature and use of the site, ambient brightness of the surrounding areas, obstructions from buildings, and landscape design are additional factors to consider. Since landscaping directly correlates to lighting effectiveness, CATALYST evaluated any landscaping interferences with lighting or normal viewing ability. The CPTED precept of "natural surveillance" promotes features which enable one's ability to view the space around them, maximize visibility, and thus increase one's awareness and reduce the vulnerability to crime. Landscaping, particularly the type of tree, shrub and/or ground cover, plant location, and growth patterns all affect one's natural surveillance and self-defense capabilities. Landscaping should not become so dense that it compromises the ability of light to penetrate or a clear line of sight. Sensible maintenance for foliage and limb removal can be achieved to balance security concerns and not disrupt the aesthetic value or atmosphere created by the landscape. During the site survey process CATALYST evaluated landscaping as it related to lighting on each campus.

There are four basic guidelines that should be employed when landscaping for natural surveillance. These guidelines are intended to provide general strategies to be considered when evaluating landscaping in specific areas. When applied with common sense, giving due consideration to both the aesthetic value of the landscaped area and the level of security required for that area, these guidelines serve to strike a balance between landscape and security philosophies.

- Ground Cover and low shrubs should be trimmed as low as possible to maintain the general landscaping philosophy of the building or area but should generally not be allowed to exceed 24" in height.
- Trees should be pruned so as to prevent branches and leaves from directly obscuring light sources (approximately 10' clear radius around light fixtures) as well as from indirectly obscuring light sources from the line of site on pedestrian walkways.
- Trees and tall shrubs should be pruned to open a clear line of site between the ground and the underside of branches. Typically, branches should be pruned to clear a minimum of 6' above the ground.

- Trees and shrubs adjacent to buildings should be pruned to allow a clear line of site between the foliage and the building (approximately 24" - 36").

During the site survey process CATALYST evaluated landscaping as it related to lighting and security. The landscaping in the parking lots and generally around the perimeter of the buildings was found to be well maintained and conducive to effective lines of sight and natural surveillance. There were, however, a limited number of areas where landscaping maintenance could be improved to heighten perceptions of safety and security. These areas are identified below:

San Jose City College Campus		
Building/Area	Location	Condition
Student Center	Staff Parking Lot	Trees limbs are obscuring fixtures
Parking Garage	Surface Lot Northeast of Garage	Trees limbs are obscuring fixtures
Fine Arts	North Parking Lot	Trees limbs are obscuring fixtures
Technology Center	North and West sides of Building	Shrubs are overgrown
Laswell Avenue	West side	Limited vegetation along roadway
Central Utility Plant	North Alley	Overgrown vegetation
Auxiliary Gym	North walkway	Overgrown shrubs and tree limbs are obscuring fixtures
Pool	North walkway	Overgrown shrubs and tree limbs are obscuring fixtures
Vocational Arts	North Quad Area	Trees limbs are obscuring fixtures
	East Side of Building	Trees limbs are obscuring fixtures
Business	East Side of Building	Trees limbs are obscuring fixtures
General Education	Quad	Trees limbs are obscuring fixtures

Evergreen Valley College Campus		
Building/Area	Location	Condition
Child Development Center	Staff Parking Lot	Trees limbs are obscuring fixtures
Parking Lot 8	General	Trees limbs are obscuring fixtures
Parking Lot 7	General	Trees limbs are obscuring fixtures
Parking Lot 6	General	Trees limbs are obscuring fixtures
Montgomery Hill Observatory	Pedestrian pathway	Shrubs and vegetation have overgrown pathway
Student Services Center	South access roadway	Trees limbs are obscuring fixtures
Cedro	West stair	Trees limbs are obscuring fixtures
Administration Offices	North Parking Lot	Trees limbs are obscuring fixtures
Parking Lot 3	General	Trees limbs are obscuring fixtures

Recommendations for improving and or rectifying the problematic areas noted above are included in Section 7 – Recommendations.

6. VULNERABILITY/RISK ANALYSIS

Programmatic, operational, procedural, and physical security recommendations are most effectively suited to the District's real security needs when based on a thorough understanding of the actual and perceived threats and vulnerabilities. Therefore, CATALYST has developed a Vulnerability/Risk Analysis, based on the findings revealed as part of this assessment.

Vulnerability/Risk Analysis (V/RA) is an effective tool used in security evaluation to systematically assess an organization's vulnerabilities and determine levels of risk resulting from these vulnerabilities. In developing a V/RA, information on various threats, both perceived and actual, is collected, evaluated, and prioritized. Information is gathered relevant to the District's policies, procedures, and systems as they apply to these threats. Finally, the prioritized list of threats and the areas of vulnerabilities are used to determine levels of risk. Recommendations can then be made to mitigate the vulnerability and thereby lower the associated level of risk. The primary goal, therefore, of the V/RA is to obtain and evaluate pertinent information such that actual and perceived threats are identified and appropriate mitigation recommendations can be made to reduce the level of risk to the District.

In addition to providing the information necessary for the development of the mitigation recommendations, a secondary goal of a V/RA is to serve as a benchmark to determine the real reduction of risk through the implementation of mitigation efforts. Over time, as threats and vulnerabilities change, a benchmark V/RA can be useful in evaluating the effectiveness of implemented mitigation efforts in reducing risks from new threats. The benchmark V/RA will often show that the application of a system, policy, or procedure to reduce a lower-risk level vulnerability will also mitigate higher-risk level, and as yet unidentified, vulnerabilities.

6.1 Definitions

Risk:

Although risk is associated with many activities, the meaning of the term *risk* in this report is limited to the uncertainty of a non-business loss. This includes the harm to staff and students, loss or destruction of physical property, and loss or damage of reputation and thereby financial stability. Risk analysis includes examining the asset vulnerability associated with the probability and criticality of the potential crime threats.

Assets:

Although risk is associated with many activities, the meaning of the term *risk* in this report will be limited to the uncertainty of a non-business loss. This includes the loss or destruction of District property, harm to students and personnel, or the loss of earned stature as an academic institution of choice. On a college campus, those loses will result from victimization crimes such as theft, vandalism, assault, sex crimes, etcetera. Risk analysis includes examining the asset vulnerability associated with the probability and criticality of the potential threats that could result in these crimes. As an initial step to identify what crimes may be possible on campus, it is relevant to define the target assets that attract those crimes.

Most campuses contain high value material such as computers, projectors, laboratory and athletic equipment, and books and materials. These items are readily recognized as valuable assets however; the physical building structures themselves and the fittings to those buildings such as lighting, telephones, landscape structures, and artwork also have replacement or repair values that can financially burden the District in the event of a loss. This is especially true for the newly installed solar panel field at Evergreen Valley College. Another key asset, and possibly the most critical, is the earned reputation of the institution. Even though of nearly irreplaceable value, this asset is often overlooked since it is not a tangible material item. Gained through the long-term effort of the institution to establish a vibrant academic atmosphere within a physically safe environment, the College reputation is arguably the key asset to protect since it is this asset that consistently and dependably attracts enrollment and tuition to the institution.

When defining the campus assets that merit security measures to ensure their viability and well-being, the reputation of the College is among the highest in value. Since the reputation asset is formed primarily from the combined resources of the employees and students that create the educational program of the institution, protection of the reputation asset is achieved as a direct result of protection of the people who attend and work at the College. Protection of the campus population is first achieved by establishing this asset as a priority within the design of the SMP. Certainly there are also valuable material assets identified for various levels of security protection, but without the student body and staff to utilize them, their value diminishes. From various perspectives, protection of the campus population is justifiable as the cornerstone of the Security Master Plan.

Likewise, the acts of theft or vandalism have a greater impact than strictly the direct material costs, since the fear of these victimization crimes is what erodes the campus

environment. As a result, total valuation of the campus material assets must be considered within the larger concept of the College's image and well-being when considering the worth of loss mitigation measures.

Based on the campus surveys, the asset groups that will be addressed in the Security Master Plan are the following:

- Reputation and standing among institutions of higher learning.
- Safety of Students and Staff as well as the security of personal information.
- High concentration areas of material value items, such as the bookstores, theatre, libraries, auto shop, and solar panel field.
- Athletic equipment – specialty training equipment, team sports equipment.
- High value electronic items – computers, monitors, audio/visual equipment.
- High value laboratory items – measuring and diagnostic equipment, specialty tools, specimens.
- Infrastructure and attractive nuisance equipment – public and emergency telephones, parking permit dispensers, vending machines, low value lab equipment.

Threats:

As discussed in the Concluding Analysis of Section 4 and recapitulated here, the District is susceptible to crime threats that can be primarily be classified as Part 1 and 2 Property Crimes (particularly Burglary, Larceny and to a lesser extent, Motor Vehicle Theft) which pose the greatest risk on the San Jose City College and Evergreen Valley College campuses.

Although not directly represented in the statistical data, but expressed by numerous College staff during surveys, is a need to increase the level of personal safety when working within their buildings, offices and classrooms. As the campus population becomes larger and more diverse, the Campus Police Department is covering a wider range of responsibilities, and the stakes for higher education are rising, some campus staff are feeling more at risk to victimization. Since statistical data is not kept on the incident rate that College staff are faced with a threatening, but non-criminal, situation within their normal work routine, the assessment relies on anecdotal information. In this case, surveys and interviews clearly indicate a population of campus staff who desire a remedy for the lack of readily accessible Police response and assistance. It should be

noted that the confidence level expressed by College staff in the Campus Police Department's ability to respond to emergency situations was fair.

Based on the combined information of statistical data and survey data, the primary threats to both San Jose City College and Evergreen Valley College are listed here in order of magnitude:

- Larceny – property theft that does not involve force or fraud
- Burglary – property theft from buildings and vehicles including forcible entry
- Non-aggravated Assault
- Vandalism
- Harassment
- Auto Burglary
- Aggravated Assault

By addressing the higher magnitude of the listed threats above, the broader spectrum of Part 1 and Part 2 offenses will also be coincidentally mitigated. Through the recommendations described in the following sections of the Security Master Plan the level of risk from all types of victimization crimes will be reduced while targeting specific known problem threats from within the campuses, as well as from the general communities surrounding them.

Probability:
Probability refers to the chance or likelihood that an incident or loss will occur, based on a proven history, the frequency of opportunity, and the target's attractive value. By using a mathematical statement to prioritize risk, probability greater than zero (no event occurs), and less than one (event definitely occurs), we develop the following scale for $1 > P > 0$:

- 0.99 = Virtual certainty that the event will occur. The event has happened before, and there is no viable impediment to reoccurrence.
- .075 = Very probable that the event will occur. The event has happened before or a clear opportunity exists, and the mitigation measures are not sufficient to prevent.
- 0.50 = An average probability exists for the event to occur. Although an opportunity exists, the event does not have an historical statistic of occurrence and any mitigation measures are incidental rather than purpose driven.
- 0.25 = A low probability exists for the event to occur. An opportunity is possible but unlikely and/or the potential target has low value.

- 0.01 = Very improbable that the event will occur. An opportunity is not present or potential target is of low value.

Criticality:
Critically measures the impact of a loss in financial terms and is corollary to business continuity. The resulting calculation reflects the importance of the loss to the survival or existence of the organization. The factor of criticality is expressed as a percentage from 0% to 100%using the following scale:

- 100% = Fatal to the organization. Total recapitalization or abandonment.
- 75% = Very serious damage to the entity. Major investment policy change, loss of life or serious injury to personnel, or major data (intellectual property) compromise.
- 50% = Average impact. An injury to personnel and/or noticeable balance sheet impact.
- 25% = No personnel injuries. Loss is covered by normal contingency reserves.
- 0% = Unimportant or irrelevant consequence.

6.2 Vulnerability Analysis

Utilizing the threats as defined above, the vulnerability analysis combines these with the factors of criticality and probability to render a product of risk (as a percentage from 0% to 100%) that can be used to guide prioritize mitigation needs in a quantifiable format.

This Security Master Plan applies the vulnerability analysis method to the most prominent offenses on campus in order to prioritize mitigation needs in a quantifiable format. The following table lists the calculations and results for the leading statistical Part 1 and Part 2 offenses:

Part 1 Offenses	**Probability**	**Criticality**	**Risk Factor**
Larceny	0.99	25%	24.8%
Burglary	0.99	25%	24.8%
Auto Burglary	0.50	25%	12.5%
Grand Theft	0.25	50%	12.5%
Aggravated Assault	0.25	75%	18.8%
Part 2 Offenses			
Non-aggravated Assault	0.99	25%	24.8%

Vandalism	0.99	25%	24.8%
Harassment	0.99	25%	24.8%
Trespassing	0.99	25%	24.8%
Traffic and Parking Violations	0.99	25%	24.8%

This data distribution shows the prioritization of offenses occurring on campus that can be used to guide the mitigation effort of the SMP. It is also clear that the categories of crime carry an approximately equal weight when allocating risk mitigation resources; and the Security Master Plan will use this equality in the rankings as the guideline for recommendations.

6.3 Susceptibility of Assets

By examining the risk factors for each of the established threats in conjunction with the assets as previously defined, the susceptibility of each asset to various risks can be determined. Below, each of the identified assets is listed with the threats that apply to that asset.

Asset:	**Susceptibility:**
Reputation	All Threats (including high criticality threats not identified due to lack of historical occurrences – homicide, robbery, arson, etc.)
Student and Staff Safety	All Threats (including high criticality threats not identified due to lack of historical occurrences – homicide, robbery, arson, etc.)
Concentration of Material Items	Burglary, Larceny, Vandalism (including high critically threats not identified due to lack of historical occurrences – Arson)
Solar Panel Field	Larceny and Vandalism
Athletic Equipment	Burglary, Larceny, Vandalism (including high critically threats not identified due to lack of historical occurrences – Arson)
High Value Electronic Items	Burglary, Larceny, Vandalism (including high

	critically threats not identified due to lack of historical occurrences – Arson)
High Value Laboratory	Burglary, Larceny, Vandalism (including high critically threats not identified due to lack of historical occurrences – Arson)
Infrastructure and Attractive Nuisance Items	Burglary, Larceny, Vandalism

This susceptibility determination is useful in developing risk mitigation recommendations as it provides a guide as to which assets can be protected by the mitigation strategy applied to counter each of the specific threats. It is worth noting that the risk factors established for each of the potential threats is relatively equal and that these risk factors are not substantially different between the two campuses, even though the surrounding communities have markedly different crime rates and Cap Index scores. As a result, the recommendations included within the next section can be uniformly applied to both campuses and the District can expect the benefit of these mitigation measures to be mutually realized at both campuses.

7. RECOMMENDATIONS

The recommendations included in this Section are based on the Crime Statistics information in Section 4, Survey Findings in Section 5, the Vulnerability/Risk Analysis in Section 6, and are applied using security industry standard best practices as found in the Protection of Asset Manual."[8] As a precursor to reviewing the recommendations, it is useful to understand the four methods used in mitigating risk.

- *Risk avoidance* eliminates an unacceptable risk to the District by removing cause of the specific risk completely. For example, the recent removal of the gamma irradiator from the campus effectively eliminated the risk that it posed. However, risk avoidance can only be applied when the cause of the risk provides little or no beneficial use to the organization.
- *Risk reduction* decreases the risk by minimizing the probability of a potential loss event through the reduction of situational criminal opportunity. This is the most commonly employed risk mitigation strategy and includes mitigation measures such as increasing lighting, locked and/or providing electronic access control devices to applicable doors, developing programs, policies and procedures directed toward increasing awareness of the employee population.
- *Risk transfer* involves moving the financial impact of a loss to an insurance company. Seemingly the easiest strategy, purchasing insurance to cover the payments to injured victims cannot compensate for the criminal act or loss of life. Also the institution may still be held responsible for negligence or civil misconduct, and the financial impact of insurance rates to cover these loses may be unfeasible. Risk transference should only be considered after the loss probabilities have been reduced as much as possible using cost effective security and safety measures.
- *Risk acceptance* is a deliberate managerial decision to accept a potential vulnerability by not taking measures to mitigate the known risk. This is a conscious administrative decision to set aside the resources to address the criticality of the potential loss. Acceptance is typically done with smaller risks having only financial consequences.

The District has employed a combination of these strategies to address many of the identified vulnerabilities, yet certain vulnerabilities are still evident. The following recommendations therefore focus on *Risk Reduction* strategies to address the remaining vulnerabilities and/or to increase the mitigating benefits of the measures currently

[8] Walsh, CPP, Timothy J., Protection of Assets Manual, The Merritt Company; 1991, Vol. 1 p.2-1

emplaced. These recommendations are divided into subsections and listed by order of priority.

7.1 Police Department Staffing and Security Command/Dispatch Center Recommendations

As mentioned in Section 5.2 – Security Program and Personnel, the current staffing levels within the District Police Department are not sufficient to effectively police the campuses and represent the greatest vulnerability to the District. In addition to the current understaffing, the non-police related responsibilities that the Department, particular Dispatch, are tasked with limit the timeliness and thereby the effectiveness of police response. Therefore, the following represents the highest priority recommendations with the SMP.

- Increase the number of sworn officers on staff to provide a minimum of one on-duty officer per campus 24 hours a day, seven days a week.
- Minimize the necessity of Officers to transit between campuses when on duty.
- Define, codify, and publish the roles and responsibilities of the District Police Department.
- Retain a bonded armored car service to collect and deposit receipts collected on campus. This includes not only parking permit machine receipts, but also all receipts that are currently deposited by College personnel.

It should also be understood that the benefits from the majority of the subsequent recommendations in this Security Master Plan, in particular, those that entail implementation and/or modification of electronic systems, will not be realized by the District unless Police staffing levels are increased and the Dispatch Center is modernized to provide effective monitoring of these systems.

Effective monitoring and control of electronic physical security systems is an essential element to a complete Security Program. The subsequently recommended Access Control and Alarm Monitoring System (ACAMS) and Video Surveillance System (VSS) can function in a stand-alone mode or in conjunction with central station monitoring. However these modes are typically used only for incident investigations and the full benefits and features of the systems will not be realized unless the systems are being actively monitored. By modernizing and staffing a Security Command/Dispatch Center (SCDC), either within the current District Police Station on the Evergreen College campus, inherent threats to District property, employees, students, and visitors can be prevented or deterred while in progress.

A fully staffed SCDC will provide the District with the ability to act in a proactive manner 24 hours a day, 7 days a week. Vulnerabilities, which otherwise would be unmitigated due to latent alarm response time, can be more effectively addressed by District Police. Additionally, police dispatch staff would have the ability to monitor the other campus and view live VSS video upon alarm call-up, allowing a more effective response to alarm conditions. Finally, the SCDC can initially be staffed during current dispatch hours and utilization of off-hour monitoring via a third party central monitoring station continued until such a time as the need is apparent for around the clock staffing. At the time of writing, the a project to remodel and expand the SCDC is planned in the near future.

7.2 Site Recommendations

Solar Panel Field

The solar panel field on the Evergreen Valley College campus represents a large financial investment for the District. Currently, with no electronic security or environmental protections in place, the field is highly susceptible to acts of larceny and vandalism. Because of the expanse of the field, fencing alone will provide little mitigation benefit. Electronically monitoring the perimeter of the field will potentially provide alarm notification upon intrusion but will be susceptible to nuisance alarms from animals within the area. While the above mitigation methods would prove to be only marginally effective, video alarm detection of the field and its perimeter would be. Video alarm detection utilizes optical and infrared camera technology and video analytics to monitor, identify and analysis intrusion into the field. When the intruder fits the profile of human, the analytics generates an alarm within the VSS that will annunciate in the SCDC. If so configured, the VSS will be able to stream recorded and live video to mobile devices carried by District Police and/or designated District personnel. It is therefore recommended that the District invest in the following to mitigate direct threats to the solar panel field:

- Video Surveillance System (scalable to accommodate future VSS needs at both campuses).
- IP based megapixel fixed and pan-tilt-zoom cameras strategically placed to monitor the field and its perimeter.
- Infrared fixed and pan-tilt-zoom cameras to support the IP cameras. Infrared cameras function equally well during the night and day and provide an added benefit when configure beside standard visual spectrum cameras.
- Required infrastructure to transmit video of solar panel field cameras to the SCDC.

Vehicle Controls

As mentioned in Sections 5.2, there are considerable safety and liability concerns regarding “on campus” vehicular traffic. While the existing roadways are necessary for deliveries, maintenance, and police traffic, general traffic and roadway accessibility needs to be substantially reduced. Additionally, parking areas that are only accessible via intra-campus roadways should be restricted to handicap parking (if required) only. The most effective method of reducing vehicular traffic through campus is with the installation of vehicle arm barrier gates. Ideally, access through these gates should be controlled via a card access reader configured within the Access Control and Alarm Monitoring System, however, considering that the recommendations within this SMP will most likely be phased in over a number of years, stand alone gate controls (for example keypads of RF opening transceivers) should be used during any interim period. Specific location where vehicle control gates should be installed and traffic strictly limited are as follows:

- San Jose City College Campus:
    - Access Road between the Student Center and Athletic fields.
    - Laswell Avenue at Moorpark Avenue and at the north end of the Student Parking Lot West of the College Union (if acceptable to the City).
    - Access road between the Auxiliary Gym and the Central Utilities Plant.

- Evergreen Valley College Campus:
    - Access road between EOP&S and Sequoia.
    - Access road between Admissions and Records and Gullo Student Center.
    - Access road from loop road to central quad West of Cedro.

Lighting

During the lighting surveys a large number of lights were found to be non-functional. Nothing, with the exception of a total absence of lighting, affects security lighting more adversely than functional fixtures with non-functioning elements. As previously mentioned, fixtures that were found to be non-functioning were marked with yellow tape. The necessity of marking these fixtures with tape was driving by the fact that there was no identifiable fixture numbering schema to effectively identify particular fixtures. As such, CATALYST has developed the following list of recommendations that can be implemented immediately.

- Replace the fixture elements that are not functioning.
- Create a campus wide lighting numbering schema and mark all campus light fixtures with a uniquely assigned number.

- Implement a reporting program that provides an easy method for faculty, staff and police department personnel to notify the Maintenance and Operations of faulty fixture.
- Implement a policy to replace any and all faulty fixture elements within a specific (and reasonable) period of time after they are reported.

Landscaping

In the performance of the campus lighting surveys, it was noted that many of the locations with poor or marginal lighting levels also had growth from tress, shrubs, and/or vines obscuring lights. These locations are included specifically in Section 5.3. Following the principles detailed Section 3.3 – Lighting and Landscaping; CATALYST recommends that the District implement the following:

- Perform landscaping maintenance to trim the foliage in the locations referenced in Section 5.3.
- Evaluate the District landscape policy with reference to Security Landscaping principles (Section 3.3) and incorporate these concepts into the regular landscape maintenance policy
- Conduct annual (in-house) campus wide landscaping surveys to identify areas that may have been missed or neglected during throughout the previous year.
- With specific reference to the West fence line along Laswell Avenue (including the East/West extension on the South side of the Technology Center parking lot) it is recommended that the District plant shrubs, similar to the ones along the South and West fence around Child Development, to reduce visibility and thereby the harassing comments directed at students by individuals through the fence.

7.3 Electronic Security System Recommendations

Access Control and Alarm Monitoring Systems (ACAMS)

ACAMS have evolved into highly sophisticated yet user-friendly tools to effectively and efficiently manage, control, and secure facilities and the surrounding site. When properly designed and installed, modern systems increase the ability to properly detect, delay and respond to potential security breeches. In general, a well developed electronic security program elevates the effectiveness of building management, increases the security of faculty, staff, students and property, and raises the effectiveness of law enforcement in apprehending and prosecuting individuals who commit crimes in and around the campuses.

The access control system, currently installed at the San Jose City College and utilized to control access at perimeter doors in the newer buildings, can be “up scaled” and utilized as the backbone of an effective ACAMS for the District. As previously mentioned in Section 5.2, this would entail: reconfiguration on the alarm points currently tied to local alarm panels so that they report directly to the ACAMS; installation of an ACAMS client workstation(s) within the Security Command/Dispatch Center; interface to single Central Station Monitoring system for after-hours monitoring and reporting of alarm events; and conversion of existing alarm points from individual buildings and classroom (at locations where access control is not financially justifiable) to the ACAMS. By creating a realistic long-term implementation strategy, the District will be able to effectively mitigate the existing local alarm systems to the centralized ACAMS, which will increase the effectiveness and timeliness in Police response to alarms and at the same time reduce the costs associated with each local alarm contract. CATALYST therefore recommends that the District begin the implementation planning for a centralized ACAMS in conjunction with a centralized Video Surveillance System and integration and expansion of the existing Emergency Communication System, which are detailed in the following sub-sections.

Video Surveillance System (VSS)

As with ACAMS, VSS have evolved in recent years and, when properly integrated, supplement the ACAMS to provide a comprehensive, event based approach to campus security. Recent enhancements in technology have revolutionized the VSS industry with the advent of network video recorders, network compatibility, ultra low light sensitive cameras, infrared cameras and direct integration with other security equipment. When properly installed and configured VSS extend the campus coverage and response while reducing staff workload and increasing staff effectiveness by providing real-time event based video in conjunction with ACAMS alarm generated events.

The backbone of the VSS is the Network Video Recorder (NVR). In addition to providing real-time event based video monitoring, NVR’s also provide ease and flexibility in reviewing video during post-event investigations, which greatly reduces the time spent on investigations while simultaneously increasing their effectiveness. Overall the NVR will deliver critical initial features for recording, playback, archival, and video file transfer as well as long-term software and hardware migration paths when the technology advances. The NVR technology also allows new and exiting analog and IP based VSS cameras to

be digitally recorded (including intelligent event recording) to single or multiple hard drive configurations as well as SANS and NAS devices that can be located remotely and accessed centrally.

Based on these considerations, CATALYST recommends that the District install a VSS, install new VSS cameras and connect existing VSS cameras to the SCDC in conjunction with the implementation planning and installation of the ACAMS.

Security Communication System (SCS)

A SCS is a vital tool in providing long-term comprehensive service and protection of faculty, staff, and students. The emergency telephones currently installed at various locations throughout both campuses have established the foundation for the SCS which the District can easily build upon.

There are currently two primary deficiencies of the existing emergency telephones. The first is that effective response after-hours cannot be guaranteed, as there is no one on campus to answer an emergency call and provide response. The deficiency can easily be rectified by providing a 7/24 police presence on each campus and programming the emergency telephones to automatically role to an “on-duty” cellular phone (carried by the on-duty officer) during the hours that Police dispatch is closed. The second deficiency is that it is, in virtually all cases, impossible to evaluate the level of the emergency from the telephone communication alone. This deficiency can be overcome through integration of the emergency telephones to the ACAMS and installation and recording of VSS cameras for each of the emergency telephone locations.

Integration of the emergency telephones to the ACAMS and VSS creates an effective SCS. When a call is initiated at an emergency telephone, an event can be simultaneously generated in the ACAMS and a live video feed from the associated camera is channeled through the VSS to a workstation in the Security Command/Dispatch center. The dispatcher can then utilize the live video in conjunction with the emergency telephone audio, to effectively evaluate the situation and direct the appropriate response. Additional, the live and recorded video feed can be streamed wirelessly to a mobile devices carried by the District Police and/or District personnel.

Based on these considerations, CATALYST recommends that the District incorporate the emergency telephones into the ACAMS and VSS, thus providing an effective SCS.

Prioritization

While the systems discussed in this Section will provide an increased level of safety and security on the San Jose/Evergreen Community College campuses, CATALYST recommends that these systems only be implemented after the recommendations in Section 7.1 – Police Department Staffing and Security Command/Dispatch Center Recommendations are implemented. The District has an obligation to provide adequate safety and security to its faculty, staff and students when on campus. Installing electronic security systems without establishing appropriate staffing levels to monitor and respond to events generated by these systems, will not only reduce their effectiveness, but it may also create a greater liability for the District then exists currently. Implementation of electronic security systems naturally increases the sense of safety and security of individuals on campus. However, if events generated by these systems are not responded to in a timely and effective manner, the perceived sense of security is found to be false and the overall perception of security on campus will be greatly diminished. Therefore, under the assumption that the recommendations on Section 7.1 are implemented, CATALYST offers the following recommendations for area specific criteria to be used in the evaluation of electronic security system implementation in New Building Construction, Existing Building Renovations, Parking Areas, and Open Campus Areas. The following subsections should be considered of equal priority and implemented in an order that is feasibly and financially practical for the District.

New Building Construction and Existing Building Renovation

The intent of the ACAMS is to provide the District with security system infrastructure that can be managed more effectively and economically. The ACAMS will provide a more secure environment for faculty, staff and students, and increase the ease with which individuals move on and through the campus. The ACAMS will also reduce the risk from theft and vandalism, thereby potentially reducing the risk of negative publicity caused by crime. Further, the ACAMS will reduce the burden on staff by providing a electronic means of locking and unlocking buildings and arming and disarming buildings and sensitive internal areas on a user definable time schedule as opposed to physically locking and unlocking doors and arming and disarming alarm panels, as is currently done throughout the majority of the campuses.

New building construction provides an excellent opportunity for the implementation of campus security systems. Yet, it should be understood that there are two primary types of architectural configurations used on college campuses and the application of electronic security systems differ between the two. The first configuration has a limited number of

outside main entrances to each building, with interior access to classrooms and labs from corridors. The second configuration has both interior and exterior entry doors to each classroom and lab. Historically, new buildings of both configurations have been equipped with burglar alarm systems that report to a third party monitoring station. Keypads included as part of these systems are used to arm and disarm the building. CATALYST recommends that use of the control keypads continues but with the migration of security alarm point field devices reporting to the ACAMS rather than local alarm panels. In addition to the keypad functionality, in architectural configurations that are financially conducive to the use of access control card readers (those with a limited number of ingress and egress routes), CATALYST recommends that perimeter access control be configured through the ACAMS with the use of access card readers and electronic locking mechanisms.

As with new building construction, the existing District campus buildings are typically of two different architectural configurations where the ACAMS criteria are unique to each. The majority of the buildings on the campuses are currently equipped with burglar alarm systems. These burglar alarm systems are from various different manufacturers, and are currently all being monitored under different third party alarm monitoring accounts. As such, CATALYST recommends that the existing alarm field devices as well as the keypads used to arm and disarm buildings and classrooms be reconfigured to report directly through the ACAMS.

With these recommendations in mind, the following lists detail specific criteria that should be considered with reference to the particular type of building considered for construction or renovation.

ACAMS Criteria – New Building Type 1 Construction (limited points of ingress/egress)

A. Install ACAMS control panels and ancillary equipment to serve as interface and control points for access control and alarm monitoring devices in the new building. Typically, the ACAMS controllers will be installed in telephone/data rooms and will be connected to and configured on a secure VLAN across the District Ethernet LAN.
B. Equip main building entrances with ACAMS card reader/keypad units, door alarm contacts, electronic locking hardware and request-to-exit devices. (Card reader/keypads will be utilized for access control and alarm zone arming and disarming.)

C. Install door alarm contacts on all perimeter doors that are not associated with card reader/keypads.
D. Install access-controlled doors with card readers to secure all telecommunication/data rooms.
E. Install access-controlled doors with card readers to secure internal areas that house any of the following physical items:
    1. Cash.
    2. Equipment of high dollar value.
    3. Potentially dangerous equipment.
    4. Hazardous equipment.
    5. Items that present an attractive nuisance.
    6. Laboratory equipment and chemicals.
    7. High value athletic equipment.

    (Note: Internal areas that will also be equipped with non-door related security devices or with doors equipped with alarm contacts only may require a card reader/keypad for internal alarm arming and disarming functionality.)
F. Secure internal areas that house any of the following data service and document items:
    1. Campus computer network equipment and infrastructure.
    2. Human Resources records.
    3. Accounts receivable records.
    4. Sensitive information that could be potentially damaging to the District if made public.

    (Note: Internal areas that will also be equipped with non-door related security devices or with doors equipped with alarm contacts only may require a card reader/keypad for internal alarm arming and disarming functionality.)
G. Provide alarm notification devices (robbery buttons) at locations where money is handled.
H. Provide security alarm devices (motion detectors, glass break detectors, etc) in interior rooms and/or areas that house any of the following items:
    1. Cash.
    2. Equipment of high dollar value.
    3. Potentially dangerous equipment.
    4. Hazardous equipment.
    5. Items that present an attractive nuisance.
    6. Laboratory equipment and chemicals.
    7. High value athletic equipment.

8. Campus computer network equipment and infrastructure.
9. Sensitive information that could be potentially damaging to the District if made public.

(Note: These types of devices are only necessary in locations that have multiple entrances and/or methods of access.)

I. Provide door alarm contacts on all electrical room and closet doors.

ACAMS Criteria – New Building Type 2 Construction (multiple points of ingress/egress)

A. Install ACAMS control panels and ancillary equipment to serve as interface and control points for access control and alarm monitoring devices in the new building. Typically, the ACAMS controllers will be installed in telephone/data rooms and will be connected to and configured on a secure VLAN across the District Ethernet LAN.

B. Install door alarm contacts on all perimeter doors and alarm keypads on the interior of the doors to provide individual alarm zone arm and disarm functionality.

C. Install access-controlled doors with card readers to secure all telecommunication/data rooms.

D. Install access-controlled doors with card readers to secure internal areas that house any of the following physical items:
    a. Cash.
    b. Equipment of high dollar value.
    c. Potentially dangerous equipment.
    d. Hazardous equipment.
    e. Items that present an attractive nuisance.
    f. Laboratory equipment and chemicals.
    g. High value athletic equipment.

    (Note: Internal areas that will also be equipped with non-door related security devices or with doors equipped with alarm contacts only may require a card reader/keypad for internal alarm arming and disarming functionality.)

E. Secure internal areas that house any of the following data service and document items:
    a. Campus computer network equipment and infrastructure.
    b. Human Resources records.
    c. Accounts receivable records.

d. Sensitive information that could be potentially damaging to the District if made public.

(Note: Internal areas that will also be equipped with non-door related security devices or with doors equipped with alarm contacts only may require a card reader/keypad for internal alarm arming and disarming functionality.)

F. Provide door alarm contacts on doors that serve as entrances to areas listed in items D and E but that are not major entrance points.

G. Provide alarm notification devices (robbery buttons) at locations where money is handled.

H. Provide security alarm devices (motion detectors, glass break detectors, etc) in interior rooms and/or areas that house any of the following items:

a. Cash.
b. Equipment of high dollar value.
c. Potentially dangerous equipment.
d. Hazardous equipment.
e. Items that present an attractive nuisance.
f. Laboratory equipment and chemicals.
g. High value athletic equipment.
h. Campus computer network equipment and infrastructure.
i. Sensitive information that could be potentially damaging to the District if made public.

(Note: These types of devices are only necessary in locations that have multiple entrances and/or methods of access.)

I. Provide door alarm contacts on all electrical room and closet doors.

ACAMS Criteria – Existing Building Type 1 Renovation (limited points of ingress/egress)

A. Consolidate campus security by replacing the existing burglar alarm panels with ACAMS control panels and ancillary equipment. The ACAMS panels will serve as interface and control points for access control and alarm monitoring devices in the new building. ACAMS controllers will be connected to and configured on a secure VLAN across the District Ethernet LAN.

B. Terminate existing alarm system field devices to the new ACAMS equipment and program accordingly.

C. Replace or reconfigure all of the existing alarm system keypads with ACAMS compatible keypads at the main entrances and interior areas.

D. Equip main building entrances with door alarm contacts, electronic locking hardware and request-to-exit devices. (Card reader/keypads will be utilized for access control and alarm zone arming and disarming).
E. Install access-controlled doors with card readers to secure all telecommunication/data rooms.
F. Install access-controlled doors with card readers to secure internal areas that house any of the following physical items:
    a. Cash.
    b. Equipment of high dollar value.
    c. Potentially dangerous equipment.
    d. Hazardous equipment.
    e. Items that present an attractive nuisance.
    f. Laboratory equipment and chemicals.
    g. High value athletic equipment.

    (Note: Internal areas that are also equipped with non-door related security devices or with doors equipped with alarm contacts only may require a card reader/keypad for internal alarm arming and disarming functionality.)
G. Secure internal areas that house any of the following data service and document items:
    a. Campus computer network equipment and infrastructure.
    b. Human Recourses records.
    c. Accounts receivable records.
    d. Sensitive information that could be potentially damaging to the District if made public.

    (Note: Internal areas that are also equipped with non-door related security devices or with doors equipped with alarm contacts only will require a card reader/keypad for internal alarm arming and disarming functionality.)
H. Provide alarm notification devices (robbery buttons) at locations where money is handled.

ACAMS Criteria – Existing Building Type 2 Renovation (multiple points of ingress/egress)

A. Replace the existing alarm panels with ACAMS control panels and ancillary equipment to serve as interface and control points for access control and alarm monitoring devices in the new building. ACAMS controllers will be connected to and configured on a secure VLAN across the District Ethernet LAN.

J. Terminate existing alarm system field devices to the new ACAMS equipment and program accordingly.
K. Replace or reconfigure all of the existing alarm system keypads ACAMS compatible keypads at the main entrances and interior areas.
L. Install access-controlled doors with card readers to secure all telecommunication/data rooms.
M. Install access-controlled doors with card readers to secure internal areas that house any of the following physical items:
    a. Cash.
    b. Equipment of high dollar value.
    c. Potentially dangerous equipment.
    d. Hazardous equipment.
    e. Items that present an attractive nuisance.
    f. Laboratory equipment and chemicals.
    g. High value athletic equipment.

    (Note: Internal areas that are also equipped with non-door related security devices or with doors equipped with alarm contacts only will require a card reader/keypad for internal alarm arming and disarming functionality.)
N. Secure internal areas that house any of the following data service and document items:
    a. Campus computer network equipment and infrastructure.
    b. Human Recourses records.
    c. Accounts receivable records.
    d. Sensitive information that could be potentially damaging to the District if made public.

    (Note: Internal areas that are also equipped with security devices will require a card reader/keypad for internal alarm arming and disarming functionality.)
O. Provide door alarm contacts on doors that serve as entrances to areas listed in items D and E but that are not major entrance points.
P. Provide alarm notification devices (robbery buttons) at locations where money is handled.

In addition to the ACAMS criteria recommendations included above, the following list detail specific criteria that should be considered with reference to VSS that should be considered regardless of the architectural building type and is applicable to both New Building Construction

VSS Criteria

A. Install NVR's in the new building. Typically, the NVR will be installed in telephone/data rooms and will be connected to and configured on a secure VLAN across the District Ethernet LAN.
B. Terminate all installed cameras (new and existing) to NVR's located within the building.
C. Configure NVR's to record cameras at a minimum of 10 frames per second at a minimum of 680x480 for existing cameras and the maximum camera resolution available new IP cameras, with a minimum storage duration of 30 calendar days.
D. Equip internal areas where cash and/or records transactions occur with high-resolution VSS cameras to view and record interactions.
E. Equip internal areas that house any of the following physical items with high resolution color VSS cameras:
    a. Equipment of high dollar value.
    b. Potentially dangerous equipment.
    c. High value laboratory equipment and specimens.
    d. High value athletic equipment.
    e. High value machinery.
    f. Attractive nuisance items.
F. Equip major building entrances and emergency exits with high-resolution color VSS cameras.
G. Equip Bookstores and retail areas with high-resolution color VSS cameras to capture areas that are conducive to shop lifting.

In addition to the installation of ACAMS and VSS at both campuses to provide heightened levels of security for faculty, staff, students and property, the need for effective communications with District Police, Operations and Maintenance, and Administration department personnel from classrooms and other internal building areas is needed. Telephones in these locations provide an effective adjunct to the Security Communications System previously described as well as the ability to allow faculty and staff to effectively communicate with appropriate departmental personnel as required. It is our understanding that telephones are installed in most non-classroom suites and departments and that they will be installed in all classrooms on both campuses in the near future. CATALYST fully concurs with this initiative and recommends that the implementation take place as soon as feasibly possible.

Parking Lots, Garages, and Intra-campus Roadways

In conjunction with the preceding building specific ACAMS and VSS recommendations, the following criteria are recommended and are applicable to campus surface parking lots, parking garages and intra-campus roadways. With specific regard to surface parking lots and parking garages, there is not sufficient risk or vulnerability present to control access into these areas. As such, the ACAMS criteria recommendations are intended to supplement the SCS and VSS location criteria.

ACAMS CRITERIA

A. Install and interface access control card readers at the vehicle control gates arms described in Section 7.2. Terminate these card readers to an ACAMS control panel in the nearest available building.
B. Where feasible, provide integration between existing SCS stations and an ACAMS control panel in the nearest available building.
C. When new SCS stations are installed, provide integration between the stations and an ACAMS control panel in the nearest available building.

VSS CRITERIA

A. Install NVR's in a secure room within the parking structure or building nearest the parking lot. The NVR will be connected to and configured on a secure VLAN across the District Ethernet LAN.
B. Install IP based color VSS cameras to view new and existing SCS stations located throughout the campuses. Resolution should be determined on a per camera basis to provide identifiable visual data to dispatchers and Police.

SCS CRITERIA

A. In new surface parking lots, install new freestanding pole SCS stations near parking permit machines.
B. In existing surface parking lots, install new freestanding pole SCS stations near each existing parking permit machine. These SCS stations can utilize the exiting power circuits for the parking permit machines and use cellular technology to minimize the need for trenching.
C. Terminate all new SCS stations to the District phone system and program to automatically call Police Dispatch when activated. Terminate the activation output relay from all new SCS stations to an ACAMS control panel in the nearest building.

Pedestrian Mall, Quads and Athletic Areas

Security requirements for Pedestrian Malls, Quads and Athletic areas are generally more difficult to define, as the application of security systems varies considerably on a location by location basis. As such, the following criteria recommendations are generalized. Specific locations and areas will need to be evaluated and defined on a case by case basis by the District.

VSS CRITERIA

A. Install NVR's in a secure room within the parking structure or building nearest the parking lot. The NVR will be connected to and configured on a secure VLAN across the District Ethernet LAN.
B. Install high-resolution color VSS cameras to view new and existing SCS stations.
C. Install high-resolution color VSS cameras to view the main use feature of the athletic areas (i.e. the swimming pool).

SCS CRITERIA

A. Install freestanding pole SCS stations along campus pedestrian malls, in quads and athletic areas at approximately 300' intervals. Size, location and use specific areas will determine the specific quantity and placement of these call stations.
B. Terminate all new SCS stations to the District phone system and program to automatically call Police Dispatch when activated. Terminate the activation output relay from all new SCS stations to an ACAMS control panel in the nearest building.

8. CONCLUSION

This Security Master Plan has utilized statistical data obtained from the FBI and CAP Index, Inc. in conjunction with information gathered during informal interviews with select faculty and staff as well as extensive site, building, lighting and landscaping surveys to prepare a detailed threat assessment and vulnerability/risk analysis and recommendations for the San Jose/Evergreen Community College District's San Jose City College and Evergreen Valley College campuses. The vulnerability and risk analysis provided a benchmark for evaluating the effectiveness of current police staffing levels, roles and responsibilities, and existing electronic physical security system. This evaluation was utilized to develop a broad range of recommendations that are intended to mitigate potential threats and reduce risk to the District, its faculty, staff, students and property. It is hoped that the prioritized list of detailed recommendations included in this Security Master Plan will serve to enhance the future vision for effective and comprehensive security and risk mitigation programs at the District.