SECURITY MASTER PLAN

For

CHABOT COLLEGE

Chabot Las Positas Community College District

Submitted by:

CATALYST
CONSULTING GROUP, INC.

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

In Association With:

DMJM, Program Management
For
Measure B Bond Program
6601 Owens Drive, Suite 238
Pleasanton, CA 94588

June 14, 2005

SECURITY MASTER PLAN

Chabot Community College

Chabot Las Positas Community College District

June 14, 2005

Table of Contents

SECURITY MASTER PLAN

Chabot Community College
Chabot Las Positas Community College District
June 14, 2005

1. Executive Summary

This Security Master Plan addresses the current findings and future vision for safety, physical security, emergency communications, and security system infrastructure at the Chabot Community College in Hayward, CA. The surveys found that the College generally has very thorough and effective security process in place, but is challenged by working with older equipment, lack of lighting, uncontrolled access, and insufficient coverage of emergency communications. The Security Master Plan presents these aspects of the safety and security program in a format that addresses the different needs of the parking lots and campus buildings, as well as an incremental approach to implementation of the recommended security systems. It is CATALYST's firm belief that the District and College commitment to the costs of site upgrades are a fully worthwhile investment in the quality of campus life, and can bring Chabot College to a par with the current standards for educational institution safety and security.

2. Introduction

Chabot Las Positas Community College District (District) engaged the services of CATALYST Consulting Group, Inc. (CATALYST) to develop a Security Master Plan for the District campuses. This report focuses on the security concerns of the Chabot College campus. A subsequent report will be submitted to the District that focuses on the Las Positas campus.

The primary intent of the Security Master Plan is to provide the District with a set of guidelines and recommendations for the selection and implementation of physical and electronic security hardware in new and existing buildings. It is further the intent of the Security Master Plan (SMP) to define campus standards for the security systems and hardware to be utilized. The security systems include the Access Control and Alarm Monitoring System, the Closed Circuit Television System (which includes video surveillance and recording), and the Security Communication System (which includes emergency call boxes, telephone, and radio-telephone interface). A Glossary of Terms and abbreviations used within this document can be found in Appendix B.

To establish the criteria and systems recommended within this SMP, CATALYST performed site surveys and conducted numerous interviews with key Chabot College staff and the Department of Campus Safety and Security, hereinafter referred to as Campus Safety. The results of these efforts

are included below and are divided into the categories of Risk and Threat Assessment, Vulnerability Analysis, Loss Prevention, Security Program, Security Operations, and Physical Security. Within these sections are details of the identified threats and vulnerabilities at Chabot College, and the recommendations that CATALYST believes will provide a sound risk mitigation program.

Since the Chabot campus will receive both new buildings and 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. However, CATALYST recommends that any future Architectural and/or Tennant Improvements to existing buildings include the security systems discussed in this SMP.

Each of the categories is introduced with explanations of the reasons used to establish the criteria, followed by a prioritized listing of the recommendations. The goal of the recommendation listing is to provide the District with a system to evaluate specific locations where new security devices will be installed utilizing an objective ranking system.

3. Statement of Scope

This Security Master Plan is an independent document incorporated by reference into the TBP Architecture District Master Plan for the Chabot College campus new construction and building improvements. The SMP uses an assessment of the campus physical and operational security measures combined with proven fundamental risk mitigation measures, and applied with current technology and policing methods to develop a long-range plan for continuous improvement of the security and safety services at Chabot College.

The Security Master Plan defines security mitigation standards that will integrate with new building construction and building improvements. By first prioritizing the identified campus risks, and then using a multi-faceted approach from the key areas of physical environment, security staffing, and feasible technology, the SMP presents the security philosophy to guide the selection and implementation of campus security upgrades. The Security Master Plan covers the areas of vulnerability analysis, security program management and operations, technological security systems, and campus physical security of buildings and grounds. The SMP is developed to address long-term system compatibility, communication infrastructure, product obsolescence, and growing demands on the security staff.

4. Project Approach

The Security Master Plan uses vulnerability and risk analysis as a foundation for developing guidelines and incorporates an assessment of current problems on campus to define the priorities for a set of risk mitigation recommendations. To develop the Security Master Plan, CATALYST has first performed numerous site surveys and interviews, analyzed crime index data, reviewed the relevant technologies, and assessed the campus physical environment to define the risks and vulnerabilities that need to be addressed for a long-term vision of campus security. From this goal set, CATALYST has developed the guidelines and recommendations for the District to standardize the approach and cost of physical security on their campuses.

The objective of the Security Master Plan recommendations and guidelines is to systematically address the following issues:

- Prioritize the identified risks on campus, and thus the budget requirements for mitigation.
- Use risk prioritization to plan mitigation measures systematically, without undisclosed expectations.
- Establish clear security goals that guide the level of implementation over the long-term.
- Provide a standardized approach to security systems to retain compatibility, knowledge basis, and functionality.

Based on this approach, the Security Master Plan will be the central document, used by the District and design teams, to establish the scope and placement of all security equipment during the planning stages of new construction or retrofit upgrade work. Using the concepts presented in the Security Master Plan the design teams will identify security system architecture and device locations for electronic hardware, access control, intrusion detection, CCTV, and security communications equipment. It is further the intent for the Security Master Plan to address risk mitigation opportunities utilizing environmental design of lighting, pathway visibility, and landscaping. The Security Master Plan will evaluate the potential threats and vulnerabilities to the District campuses, and develop a security program incorporating electronic, programmatic and physical security measures as required to achieve acceptable levels of risk mitigation that can function in harmony with students, campus employees, and District service providers.

A key source of information used in master plan preparation is data collected during site surveys and interviews regarding perceived threats and vulnerabilities. A survey of currently implemented risk mitigation measures was used to assess the extent of applied physical security methods and their effectiveness. Interviews were conducted to gauge the overall impression of campus security by the people who attend the college. Interviews with facility and departmental personnel provided insight

into whether the physical security mitigation measures were in line with the personnel's perceived level of vulnerability.

The methodological approach to the survey process divided each facility into three target areas: site perimeter and surrounding area, building perimeter, and sensitive internal areas. A list of the general investigation points for each target area follows:

Campus Site and Surrounding Areas:

- Paths and proximity of vehicular and pedestrian traffic
- Vehicular and pedestrian points of access
- Site fencing and landscaping
- Site lighting, including nighttime lighting level measurements
- Existing physical security systems (access control, CCTV, etc.)

Building Perimeter:

- Paths and proximity of vehicular and pedestrian traffic
- Points of access and locking systems
- Landscaping along the perimeter
- Perimeter lighting, including nighttime lighting level measurements
- Existing physical security systems (access control, CCTV, instruction detection etc.)

Sensitive Internal Areas:

- Points of access and locking systems
- Public accessibility
- Existing physical security systems (access control, CCTV, instruction detection, panic alarm devices, etc.)

During the site interviews, CATALYST's objective was to gather perceptions of vulnerability in relation to the existing physical mitigation measures. The interviews were intentional informal and designed to establish an open dialog regarding the following:

- Existing physical security systems
- Expectations for usefulness and effectiveness of new physical security systems
- Perceived vulnerabilities of personnel
- Perceived vulnerabilities of assets

- Perceived level of effectiveness of security staffing
- Awareness of various threats and vulnerabilities

CATALYST has also collected various statistical data representative of crime levels in adjacent communities. Using the Uniform Crime Reporting Index (UCR) and CAP Index reporting, CATALYST extrapolated crime threat levels relevant to the particular campus as it exists with the community. The statistical data provided an analysis of local county and neighborhood crime levels compared to national incident statistics.

5. Risk Analysis and Threat Assessment

5.1. Asset Definition

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 campus physical property, harm to campus 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, or other. 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 valuable books. 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. 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 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 Security Master Plan. 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 damage 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 primary asset groups that will be addressed in the Security Master Plan are the following:

- Campus personnel – Students and staff.
- High concentration areas of material value items, such as the Bookstore, theatre, library, and auto shop.
- High value electronic items – computers, terminals, AV equipment.
- High value laboratory items – measuring and diagnostic equipment, specialty tools.
- Athletic equipment – specialty training equipment, team sports equipment.
- Infrastructure and attractive nuisance equipment – public and emergency telephones, ticket dispensers, vending machines, low value lab equipment.

5.2. Threat Assessment

Threat assessment begins with threat identification. 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[1] 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

[1] Pearson, F.S. and J. Toby (1991). "Fear of School-Related Predatory Crime." *Sociology and Social Research.*

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[2] found that in general, community crime rates and characteristics had little effect on campus crime.

In fact, the characteristics of the 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. The Security Master Plan will therefore mitigate the threats of robbery and auto theft uniquely as threats from outside the campus by using a combination of increased lighting in key areas, vehicle entry and exit control, and parking lot video surveillance. It is essential to note that if the parking lot video surveillance is intended for any purpose other than after the fact evidence investigation, then the video system and parking areas must have 24/7 monitoring. Without this level of monitoring, the District can potentially be held liable for maintaining a video system that was believed to provide protective security when in fact it really does not.

Using the Campus Security Act statistics from the College Safety Department, we can historically identify the threats that have targeted Chabot College. Accounting for 92% of the total of Part 1 Offenses for 2004, the three areas of petty theft, auto burglary, and vehicle theft rank as the crimes with the highest occurrence rates; past statistical data and the site surveys also indicated these crimes are the main concern to the College as the threats needing attention in the Master Plan. In addition, Part 2 Offenses are historically dominated by vandalism, disturbances, simple assault, and traffic/hit-and-run violations making up 82% of this crime bracket. While assessing statistical data is valuable, the Security Master Plan will also factor in new information on the current conditions evident from surveys and interviews in order to focus risk mitigation efforts to the areas of greatest need.

Although not directly represented in the statistical data, but expressed by numerous campus staff during site meetings, is a need to increase the level of personal safety when working within their offices or classrooms. As the campus population becomes larger and more diverse, Campus Safety is covering a wider range of responsibilities, and the stakes for higher education are rising, certain campus staff is feeling more at risk to victimization. Since statistical data is not kept on the incident rate that College staff are faced with a threatening situation within their normal work routine, the

[2] Lizotte, A.J. and A. Fernandez (1995) *Trends and Correlates of Campus Crime: A General Report.*

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 emergency communications.

The primary concern is for a more readily accessible voice communications system, as well as emergency duress buttons for certain locations where urgency is essential to alerting Campus Safety to a threatening situation. CATALYST also believes that difficulty or delay in initiating an emergency notification is a vulnerability, and in fact could be a liability for the College and District based on new school construction standards, where by comparison, telephones are installed in classrooms. The need for emergency communications is especially true for those staff that directly interface with students in counseling, financial aid, registration, and administration, and who are concerned about being vulnerable to a threat from an agitated individual within their work space. There is also no emergency communications for campus staff in the locations that handle cash.

CATALYST recommends improving the capability for emergency notification, and the details of the Security Communications System needs are addressed in the Physical Security section of this report.

Based on the combined information of statistical data and survey data, the threats to Cabot College campus are listed here in order of magnitude:

- Petty Theft
- Auto Theft
- Emergency Assistance Communications, including Duress/Panic Alarms
- College property theft, including A-V, electronic, and theatrical stage equipment
- Auto Burglary
- Vandalism

By addressing the highest 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 campus, as well as from the general community of Hayward.

6. Vulnerability Analysis

The process of vulnerability analysis combines the factors of criticality and probability to render a product of risk that can be used to guide the investment of mitigation measures. *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 $0 < P < 1$:

- 0.999 = 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.
- 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.
- .025 = A low probability exists for the event to occur. An opportunity is possible but unlikely and the potential target has low value.
- 0.001 = Very improbable that the event will occur. An opportunity is not present or potential target is low value.

Criticality measures the impact of a loss in financial terms. The resulting calculation reflects the importance of the loss to the survival or existence of the *institution or organization.* The factor of criticality can be expressed 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, major data compromise.
- 50 = Average impact. An injury to personnel, noticeable balance sheet impact.
- 25 = No personnel injuries. Loss is covered by normal contingency reserves.
- 0 = Unimportant or irrelevant consequence.

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**
Petty Theft	0.99	25%	24.8%
Motor Vehicle Theft	0.75	25%	18.8%
Auto Burglary	0.75	25%	18.8%
Grand Theft	0.75	50%	37.5%
Deadly Weapon Assault	0.75	50%	37.5%
Burglary	0.75	25%	18.8%

Part 2 Offenses			
Vandalism	0.99	25%	24.8%
Disturbances	0.99	25%	24.8%
Fraud and Forgery	0.75	25%	18.8%
Trespassing	0.99	25%	24.8%
Traffic and Parking Violations	0.99	25%	24.8%
Threats	0.99	25%	24.8%
Restraining Order Violation	0.75	25%	18.8%

By including the factor for known statistical occurrence[3] of each event and recalculating the table, the threats can be ranked in order of the adjusted risk factor. The adjusted risk factor is the product of the statistical occurrence of the offense and the calculated risk factor, and indicates the relative occurrence of the highest to least risk offenses.

Rank	Part 1& 2 Offenses	Probability	Criticality	Risk Factor	Statistical Occurrence	Adjusted Risk Factor
1	Petty Theft	0.99	25%	24.8%	0.540	13.4%
2	Vandalism	0.99	25%	24.8%	0.300	7.4%
3	Motor Vehicle Theft	0.75	25%	18.8%	0.240	4.5%
4	Disturbances	0.99	25%	24.8%	0.170	4.2%
5	Auto Burglary	0.75	25%	18.8%	0.140	2.6%
6	Trespassing	0.99	25%	24.8%	0.096	2.4%
7	Fraud and Forgery	0.75	25%	18.8%	0.120	2.3%
8	Traffic and Parking Violations	0.99	25%	24.8%	0.089	2.2%
9	Grand Theft	0.75	50%	37.5%	0.056	2.1%
10	Threats	0.99	25%	24.8%	0.052	1.3%
11	Deadly Weapon Assault	0.75	50%	37.5%	0.016	0.6%
12	Burglary	0.75	25%	18.8%	0.016	0.3%
13	Restraining Order Violation	0.75	25%	18.8%	0.012	0.2%

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 worth noting that "Disturbances" which are ranked 4th in risk, is a compilation of offenses that could also be distributed separately to their own categories, but as a whole require security department resources to address this group of offenses at a higher probability than attending to another offense that carries a higher risk. If the "Disturbances" category is excepted from the discussion, auto burglary, trespassing, fraud/forgery, grand theft, and traffic violations all rank in a very close 4th place. This implies that these five categories of crime carry an

[3] Chabot Community College 2004 Crime Statistics – Appendix I

approximately equal weight when allocating risk mitigation resources; and the Security Master Plan will use this ranking as the guideline for recommendations.

Based on the site surveys and interviews it was also determined that auto theft has increased dramatically in the 2003-2004 period, with a rash of approximately 15 cars being stolen in a single 2003 semester. The statistical incidence of petty theft is obviously much higher than the incidence of auto theft; however the petty thefts are occurring where a concentration of valuable items is located, such as the bookstore or A-V labs. Although there is great concern about these thefts, the losses are directly affecting a select number of the campus students and staff, not the bulk of the campus population. The crime of auto theft on the other hand affects a much wider cross-section of the campus and is personally felt by the victims. Auto theft also has the broader affect of creating the sense of an unsafe environment that goes beyond the direct representation of criticality statistics. Since it is a primary tenet of the Security Master Plan to alleviate the sense of an unsafe environment, significant steps to improve the parking lot security such as increased lighting, CCTV, expanded assistance phone coverage, and vehicle entry control are recommended for long-term improvement of campus safety. These recommendations are detailed in the Physical Security section of this report.

7. Loss Prevention

It is necessary to use the entire replacement cost of an item to accurately evaluate returning the lost service or feature to its previous condition. This not only includes the new purchase price, but also the delivery cost, installation cost, and possible costs for a temporary replacement of the original item. There may also be indirect costs such as downtime when the institution cannot fulfill its normal service obligation to students and the community. Additionally, if an insurance claim must be filed due to the loss, there may be a recalculation of the risk, resulting in adjustments to the insurance rates paid by the institution. Since the top ten risks on campus are related to property crimes, the concept of total replacement cost is directly relevant to selecting the distribution of strategies for risk management. The Security Master Plan will apply a *risk reduction* strategy as the primary method of lessening the risk to Chabot College, although ultimately the overall strategy will include a combination of risk avoidance, transfer, and acceptance depending on the decisions of Chabot College and the District.

Presented in brief, the strategies that will work in conjunction with the SMP are the following:

- *Risk avoidance* eliminates an unacceptable risk to the campus population by removing it completely from the campus. For example, it may be in the best long-term interest of the

institution to close a thoroughfare street or high-risk portion of the facility rather than attempt to manage the risk.

- *Risk reduction* decreases the risk by minimizing the probability of a potential loss event through the reduction of situational criminal opportunity by increasing lighting, keeping doors locked or access controlled, and increasing the awareness of campus personnel to make them less of a target.
- *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 lost 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, such as the loss of some definable value of textbooks, AV equipment, or other program material where replacement items are readily available.

Like most institutions Chabot cannot employ only one risk management strategy to cover all contingencies, rather there will be a combination of strategies used to effectively address the identified vulnerabilities. This will include removal and avoidance if possible, risk reduction by increasing safety and security standards, insurance for the risks that cannot be made less critical, and acceptance of the risks that the institution can live with.

8. Security Program Management

8.1. System Life-Cycle Ownership

The introduction of access control, CCTV, and other technologies into security operations will alter the security operator's interface to their environment, not unlike factory automation removes the operator from directly turning valves or operating other field equipment. This inherently changes the current landscape by bringing the security operator into contact with a new computer interface, as well as increasing the demands of the associated facility resources to support this new software environment.

When considering the installation of software and network based solutions, possibly the most important factor for successful long-term operation is clearly establishing the systems administration

responsibilities to oversee the functional use, network loading, application deployment, and periodic maintenance during the product's life-cycle. Typically one individual will not perform all administration at all levels, and Chabot College and the District are similar in this regard. Rather there will likely be a hierarchy of system administrators, or area managers, each managing their own functional tier but working in concert within common network and software usage rules for the campus security systems and District IT standards. Even with area management functions being allocated to the best available resource, CATALYST also believes that a key administrator is needed to manage and coordinate the available resources to support ongoing operation as well as certain aspects of systems usage. In the SMP, this is the Security Systems Administrator.

Since these key individuals are not currently named, a process is needed at the College and District to define management and service functions, and allocate the appropriate head-count to accomplish those responsibilities. The most favorable time to identify the all the key individuals and their roles is before the systems are installed to better ensure that all the desired features are activated, and a firm knowledgebase of systems operation is established early on. Although the process of systems administration is not necessarily an IT department role, virtually all modern security systems are software-based, and communicate over an existing LAN or dedicated security LAN. As such, it is imperative that the Security System Administrator and the IT department have a close integration and working status with the departmental systems administrators at all levels. Any new system software will also come with software licensing, and a process within CLPCCD needs to be initiated to clarify who is designated as the central repository for licensing from each system.

Since the security systems affect the safety and well-being of the entire campus population, establishing the Security Systems Administrator must be approved at the top level of campus administration so that there is no question regarding the importance of campus security or authority of its management. This is especially true of the access control system which will contain information for all cardholders within the system database. Any access control system will also effect a change to the normal routines of ingress and egress, so planning early for a smooth implementation of the administrative assignments will directly affect the short and long-term acceptance of the system.

Based on the College and District desire to decentralize system administration, some typical responsibilities listed below would need to be allocated accordingly:

- Identify at least one key alternate Security System Administrator.
- Establish and maintain the business rules for networked systems use in accordance with the manufacturer's recommendations and CLPCCD network standards.

- Be the coordinating contact on campus for warranties, service agreements, software licensing, and software updates.
- Be the primary person to receive system training, and define the scope of which individuals or departments are also trained for system operations.
- Define the scope of responsibility within each department or user group for adding/deleting cardholders, or for changing access schedules and levels.
- Establish the campus policies and methods for issuing access cards.
- Load software updates and patches.
- Address system user questions – Help Desk Support.

On the Chabot campus, the access control system users (cardholders) will be College employees, although there may be some exceptions for students, student aids or other users with authorized access to certain parts of the campus and/or parking lots. Since most of the users are employees, and their records are typically maintained in the Human Resources department, it is not unlikely that the HR department would have an area manager or even a co-administrative role. Campus employee badge issuing would also be handled in HR. Acting as a co-administrator, this HR person would also have direct communications with Campus Safety, the various department heads, and the IT department. Campus safety is notified by email or other recorded communication of database deletions due to termination, and department heads can be granted authorization to perform the cardholder add and delete functions as their staff changes.

While there are certainly other duties that the Security System Administrator will perform over the life of the systems and in conjunction with the above items, the primary issue is identifying and installing this individual as the key component to the total viability of the security systems. Experience has shown that the most successful security systems have an administrator that serves as a single point of contact for both outside vendors and on-campus liaison. This individual should be available to dedicate their primary attention during the initial start up, and for some time following. Similar to most software-based solutions, once the security systems have been operating long enough for the users to gain familiarity, the Security Systems Administrator's immediate demands are decreased and their attention can be focused on system optimization rather than troubleshooting.

a. Daily Operations

Access control - Once the user database is established and cards are issued, the daily operations of the campus security systems will be primarily the responsibility of Campus Safety. The access control system does not require 24/7 staffing; however a client user interface is typical for utilizing the system features. Full time staffing is especially important for alarms generated through the monitoring capabilities of the access control system. Some of the typical functions available to a client user are:

- Alarm monitoring
- Confirming badge validity
- Preparing access reports for door or badge activity
- Remote lock or unlock of doors
- Departmental adjustment of time schedules or access levels

Currently building doors on campus are locked and unlocked by safety or maintenance personnel. This process takes time, can be faulty or inaccurate, does not have traceability, and is subject to violation through key theft. The access control system has the capability to lock and unlock building exterior doors on a programmed schedule, as well as accept card read access for additional doors that lead directly to classrooms, high value instructional rooms, or building main entry doors during off-scheduled hours. Based on the evaluation of Campus Safety operations at Chabot College and an understanding of the variability of the college class scheduling, CATALYST believes the most successful system architecture for the access control system will include a client user within Campus Safety and Security, a client user for each department head, and an administrative user as designated by Chabot College. The software and database maintenance can be performed by IT or through contract agreements, and the field devices such as door locks, card readers, and motion sensors can be maintained as they are currently unless the College desires to engage an outside contractor.

CCTV & Video Surveillance – There is a Closed Circuit Television (CCTV) system within the bookstore, however there is currently no actively monitored video surveillance for the campus. Auto theft, auto burglaries, and vandalism, along with a limited capacity for Campus Safety personnel to cover the entire campus at once have highlighted the need and value of deploying a CCTV solution at Chabot. CCTV will be used as a risk reduction strategy to mitigate the statistical crime and sense of fear that is caused by the parking lot crime as well as reduce the ease of vandalism to occur undetected. Daily operation of the campus video system will be the responsibility of Campus Safety. Since Campus Safety is the primary user, they will also be responsible for training their personnel, warranties, and service agreements. Modern video recording systems communicate over Ethernet; therefore IT will need an understanding of the client-server relationships over the network and bandwidth utilization requirements. Software licensing and software updates will likely be managed by IT as well. It is conceivable that the periodic maintenance of the video system can be performed within the facilities M&O department, or the required maintenance can be performed through service agreements with contractors. In either case, the video system cannot perform indefinitely without some maintenance so that a defined source for this service needs to be established early in the system design.

Emergency Communications – Operational responsibility of the emergency communications systems, radios, call boxes, and dial telephones, is virtually identical to the video system in that Campus Safety is the primary user and system maintenance can be managed by Chabot College M&O or a contracted through an outside service provider. Typically service is handled on a tiered basis, with basic problems evaluated first by site technicians, then escalated to factory support if required.

8.2. Security Staffing and Training

Feeling safe on campus affects the overall quality of the education, and is interrelated to student recruitment, retention, and ultimately financial viability of the institution. During the site surveys, the Campus Safety staff appeared professional, competent, and helpful, so clearly understands their direct impact on the success of the institution. Then Campus Safety staff generally exhibits the evolution of campus security from earlier roles of primarily property protection to the more current roles of professional policing with humanist orientation. As is clearly stated in the Chabot College Campus Safety and Security webpage, the security staff receives continuing professional training in first aid, CPR, emergency response, disaster preparedness, safety, and security each year. It is imperative that this training continue as new staff is brought on and policing methods advance. Using problem-solving policing methods, Campus Safety staff works closely with the campus community to identify problems before they escalate into crime or disorder. In the campus environment, once the crime has been committed, little can be done in the short-term to remedy the fear and apprehension. So, different from the traditional community policing approach of criminal apprehension, the campus security focuses on crime prevention through their relationships on campus.

It is safe to say that most departments could provide better service with a larger staff, and Campus Safety is no exception. An increased number of patrol officers could cover more of the parking lots and campus buildings, yet without excess staffing Campus Safety has a definite presence on campus both day and night. The Department of Campus Safety and Security is directed by a sworn police sergeant from the city of Hayward, and has a staff consisting of a sworn Hayward police officer, civilian campus safety officers, dispatchers, on-call campus safety officers, and student cadets. In the event of a hostile action on campus, it is conceivable that the campus staff would not be sufficiently sized depending on the magnitude of the disturbance. However, Chabot College has a well established working and contractual relationship with the local Hayward police jurisdiction and could utilize this resource directly in the event of an emergency. CATALYST did not find a need to expand the Campus Safety staff at this time, although depending on the scope of the security control center, additional staff may be required in order to accomplish the desired level of service.

8.3. Security Control Center – SCC

a. Operational Requirements

As part of the District goals for security master planning, there is a desire to create a security control center to serve both the Chabot and Las Positas community colleges. There has been some discussion on whether the control centers should be separate or combined, and if combined what the common services would be. Given today's communications technology and networking capabilities for data, and video, there are numerous sound reasons to combine the services in a single location – cost and efficiency being at the top. Conversely, two separate control rooms offer a measure of redundancy in the event of power or communications loss at the single location. Although redundancy has some value, CATALYST believes that the District can more feasibly revert to the current level of security system infrastructure in the event of a control center failure rather than validate the cost or necessity of service duplication. CATALYST believes that a single control center offers the following advantages:

- A smaller pool of trained control center operators is required.
- Video data can be stored and managed on a single server.
- Access control data can be stored and managed on a single server.
- Site alarm monitoring (currently Sonitrol) for both sites can be assumed by the security control center.
- Head end communications, access control, and video system components do not have redundant costs.
- Control center construction costs are less.
- Service agreement contracts are only required for one location.

CATALYST therefore recommends that a single control center be utilized to service both Chabot and Las Positas campuses. The control center can have the following operational functionality:

1. Standard C.O. multi-line phone capability, with direct interconnect between Chabot and Las Positas security offices.
2. Emergency telephone communications for connectivity with all site emergency call boxes.
3. Radio-Telephone Interconnect system for communications with patrol officers and emergency phone system, or stand-alone radio and stand-alone emergency call systems.
4. Client workstation PC for connectivity to college LAN and email communication.

5. Client workstation PC for connectivity to access control and alarm monitoring system server (ACAMS).
6. Client workstation PC for connectivity to campus all-call system.
7. Video display PC and screen for monitoring video surveillance system.
8. Ergonomic workstation structure and lighting

At this time a room and location for the SCC has not been selected or designated on the College campus. This will need to be determined as a joint Administrative, Campus Safety, IT/Communications, and architectural decision.

b. Technology Requirements

The technology requirements for the security control center will need to support the above described systems with the current District standards for network communications, and include District firewall, anti-virus protection, software patches, and password protected log-on requirements. PC power and operating systems must meet minimum standards set by the manufacturer of each system, and be compatible with District network standards for operating systems. All computer monitors will be flat panel LCD monitors; voice equipment for the radio systems will use the current technology available for control room dispatch and public safety systems.

A back-up source of power is recommended to supply critical SCC equipment and emergency lighting. Individual system servers and PC's must have back up power and can use dedicated stand-alone UPS for a short duration of power outage, however there needs to be an emergency source of power available to serve the SCC in the event of a long-term loss of power. This does not necessarily require a permanent back up generator, but at least the ability to connect to a source of emergency power. Back up power requirements for the SCC are independent of the power requirements for the District Data Center which is only planned for support of the network core in the event of a utility power failure.

The SCC will be designed for environmental consideration of HVAC and lighting, and control room furniture will be engineered to meet ergonomic standards and designed for commercial application.

8.4. Security Awareness Training

The College's position on security awareness training can most readily be found as public service information on the Chabot College *Department of Campus Safety and Security* webpage. This page within the Chabot College website points out crime prevention tips, security policy, and lists the various processes that are used at Chabot to reduce risk. The College is taking a pro-active position by thoroughly describing their safety programs, the mitigation measures, and the philosophy that

clearly indicates that Campus Safety is dedicated to serving the college community and providing a safe and prepared campus.

Within the Campus Safety webpage is an extensive description of the security awareness and training programs that are sponsored by the Department and that are available to all members of the college community. Campus Safety also utilizes the campus newspaper to distribute up to date information on personal safety, crime trends, or relevant incidents that pose a threat. CATALYST believes that Campus Safety is providing a very comprehensive and professional approach to educating the college community on security awareness and personal safety, and recommends that Chabot's process be used as the District model for orientation and training. CATALYST recommends that Campus Safety continue to utilize its resources within the student body and college staff to gauge the effectiveness of their communication methods.

9. Security Operations

9.1. Badging

a. Badge Issuing

The term "badge" is used to describe the plastic credit-card like credential, sometimes called a "card-key". The badge in today's ACAMS is capable of being used as an electronic key to open doors, as well as identification with storage of a wide variety of information bases such as HR, student expenses, and integration with Blackboard or other educational management systems. Badge issuing, or "badging", or "badge printing" is preceded by first establishing the accepted appearance of the badge, usually including the institution's logo, determining the appropriate picture size, graphical borders, etc. Once these decisions are final, the badge template can be set up by the badge system manager, and issuing can begin. The primary users of access control badges on campus will be employees. Campus employees can be issued access control badges through Human Resources, with the access levels and authorizations established by each department. This will give flexibility at the department level to accommodate temporary or short-term teaching staff, as well as having direct responsibility for badge deletion from the database. Since the building main entry doors will be equipped with card readers, issuance of access badges to allow entry into building perimeter doors will greatly reduce the risk from lost or non-returned keys. Key issue will only be required for specific classroom doors, so will not need to be sub-master level keys.

b. Badging Systems Management

Badge system management requires a convenient location on campus where photos can be taken and the badges can be printed. A PC workstation is required to configure the badge template and control the photo/printing process. Badge system management does not require administrative access to the system, so can be performed by an individual designated by the security System Administrator. It was presented previously that the administrator is sometimes selected from the HR department, and likewise, badge system management can readily be performed in this department due to familiarity with the information required to program each badge. However, the assignment of these positions is best done by the College, and well before the implementation of the badge issue.

Since some time is involved in photos and data entry, the initial phase of new badge issuing should be planned for completion at least 1-2 weeks prior to the commissioning of the access control system. It is also very effective to use a third party contractor for the initial badging issue, working in conjunction with HR personnel where additional badge printers can be brought on site, and the badging time span is compressed considerably.

c. Visitor Badging

Control of visitor access can be handled in a number of ways, but certainly it is easier and more accurate when utilizing the ACAMS. One of the simplest methods is to have the ACAMS equipped with a visitor management module that allows an email request to Campus Safety or the badge manager to create a record with the visitor's information. This record can be pre-programmed to permit access to specific areas, and have a definite expiration time. When the visitor arrives on campus, they proceed to the Campus Safety Office to pick up their badge and any special instructions for their visit. The visitor is issued a temporary "soft" plastic badge that allows electronic access control, but does not have a photo, and is not intended to have the same durability as a permanent badge. This would be the standard process for an invitee to the campus, but is essentially the same for a vendor or contractor that has a finite period of service to the College. When the visitor has completed their time on campus, the badge can be dropped in a conveniently located repository. Or if the visitor forgets to deposit the temporary badge, it has a relatively low cost so not a significant impact.

d. Staff and Student Badging

The primary users of the access control system will be the College staff; therefore this group will be the majority of the access card holders. Access cards will be issued as described in 9.1a, with the card being provided through the Human Resources Department. The student population can also benefit from the badging system through the process of student ID card issue. In the latter section on

Parking Lots, CATALYST recommends the use of access control to mitigate the risks of auto theft, and student badging is a key part of the solution. A method utilized on various college campuses incorporates the student ID process with issuing access control cards to those students who also have access to parking. When students register for class they are offered the access to parking and can be issued an access control card with the student ID laminate face. The card will be programmed for access into certain parking lots, or other locations as authorized. Those students that do not wish to have the parking access are issued an identical looking card, however not electronically enhanced.

To accomplish greater control of the parking lots, as much as possible of the student population who are parking lot users will need to have an access control card. This will increase the amount of the parking spaces (lots) that can use card access for entry, thereby reducing the amount of uncontrolled flow through the parking lots.

9.2. Access Control and Alarm Monitoring System (ACAMS) - Operations

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 employees and information, and raises the effectiveness of law enforcement in apprehending and prosecuting individuals who commit crimes in and around the facilities.

The fundamental network architecture for the ACAMS is a server and some number of user clients, including the badging station. After installation and programming of the ACAMS the College will have the communication backbone to provide security devices and effective monitoring of both new and existing buildings, on both Chabot and Las Positas campuses. It is recommended to the District that all future building renovation and new construction include security field panels and devices that communicate with and are controlled by the new ACAMS server with the goal of converting all District facilities to a single integrated system over the next few years. This makes the most sense for effective monitoring and control from a single location, as well as the management of a single software package. Those buildings that are currently have alarm monitoring can be consolidated through the ACAMS to output a single account to the central station. This will reduce the cost of monitoring numerous individual accounts until the security control center is built out and staffed. It will then be possible to migrate all of the alarm monitoring to the SCC and discontinue the central station service. In the meantime, the ACAMS will be programmed to communicate with a third party alarm

monitoring company to notify Campus Safety of after hours alarms from any of the buildings equipped with the new ACAMS.

Understanding that there may be locations where the criteria for ACAMS card readers are not justified but a level of security above mechanical keys is desired, CATALYST recommends that the District establish standards for electronic, stand-alone door control hardware, typically referred to as "Cyber locks", and not to be confused with keypad or pin-code locks that have very low security protection. Cyber lock systems typically use passive electronic cards or key fobs to control access. Since the stand-alone locks do not report back to the ACAMS server on real time, they also do not provide a level of security on par with an ACAMS. However, these locks do allow for an effective single point of controlling access privileges without use of a key, and retaining a historical activity record that can be downloaded from each lock. Each unit is programmed with an individual identity code similar to the facility card readers. Cards or fobs are typically programmed at a centralized location such as the badging station. The cards or fobs can be programmed with expiration dates and times so that key control can be more effectively managed. Additionally, if cards or fobs are lost, the unit memory at the door locations can be erased without incurring the expense of re-keying doors. Finally, the District may choose to incorporate Cyber Locks within existing buildings to increase the level of physical security until the time when funds are available to renovate the existing security system within the building. Because of these features and the inherent advantage over mechanical keying systems, CATALYST believes that a Cyber lock system is an effective adjunct to the Districts ACAMS.

9.3. Key Control

Mechanical locks are the most common mechanisms for access control on doors and secured containers. They are found in the vast majority of residences, commercial businesses, educational institutions, and government facilities, and often serve as the primary protection against intrusion and theft. The justifications for this choice include low cost, simplicity of operation and reliability. All of these benefits will be negated however, if the locking systems are not efficiently planned and administered. The loss of a master key requires the replacement of all key cylinders within a facility at a potential cost of thousands of dollars. Similarly, the lack of control over key issuance and more importantly the return of keys could cost an organization an inordinate amount of money due to loss of assets, theft or destruction.

In a recent research paper, *"Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"* January 27, 2003, Matt Blaze of AT&T Research Labs, demonstrates that virtually all master keyed mechanical lock systems are vulnerable and a duplicate master key can be easily produced. The research paper can be downloaded from the Internet and is readily available to any

person. Creating a duplicate master key requires no special skill, leaves behind no evidence, and does not require engaging in recognizably suspicious behavior. The only materials required are a metal file and a small number of blank keys, which are easily obtained. Unfortunately, there is no simple or completely effective countermeasure that prevents exploitation of this vulnerability short of replacing a master keyed system with a non-mastered one or installation of an electronic access control system.

It is at the employee level that the lock and key system can be compromised. While Chabot has a policy, which states that all school property shall be returned upon termination or change in employment status, it is not clear that this policy is effective in getting all keys returned. Specifically, keys are often not returned by the former faculty member or staff prior to leaving employment by the College. Perpetual and chronic failure to have sub-master and office keys returned by employees has resulted in a condition in which the College cannot be certain who has keys to specific buildings, equipment rooms, offices, or other places in which confidential information or assets are stored. When the elements of a key control program are compromised in an organization, re-keying a facility can be an ineffective and endless measure.

Deployment of the ACAMS significantly reduces the cost, management, and liability of key system control. As described below in the section on Physical Security Recommendations, electronic access control will be applied to building main entries and high-value locations. For the typical users in the faculty, this leaves only the key to the classroom and possibly an office key remaining. The requirement to issue a sub-master key to allow building entry is no longer required. As a general rule, all the standard methods of key control policy should still be applied to manage those keys which are still in circulation. Such methods include:

- A well-constructed cabinet is required, of sufficient size to hold the original keys for all locks, extra keys, key blanks, and any additional keys that are in use at the College. The cabinet should be installed in such a manner so as to be difficult, if not impossible, to be removed from the property. The key to the key cabinet must receive special and limited handling, and should be maintained inside a combination-type safe.
- A key control administrator (typically the Maintenance Manager) oversees the key control program. The key control administrator maintains a record of the permanent issuance of keys and signed recipients. Additionally, a log should be kept and monitored by the key control administrator for signing in and out keys that are issued and returned on a daily basis.
- All employees should be informed that duplication of keys is not permitted and the loss of keys should be reported immediately.

- The College must recover keys from personnel who are no longer employed by the College or District. Some organizations add this to the list of items to be processed in the exit interview.
- All master keys should be numbered for control and accountability purposes.
- All keys should be stamped or engraved with a number for identification and accountability purposes and stamped "Do Not Duplicate". The record should be protected as a confidential document.
- Conduct periodic inventories to verify that all keys are accounted for and are still in possession of the employee to whom they have been issued.
- It is important that Chabot College administrative and academic management, at all levels, lend positive support for the program and enforce handling procedures.
- Optionally, to achieve a quality key control program, it is suggested that each month one section or department be scheduled for lock changing and re-keying. A monthly program spreads the cost and work efforts throughout the year and permits prioritizing areas for retrofitting. Coupled with deployment of ACAMS, this will eventually reduce the key system management costs significantly.

9.4. Bookstore Theft and Loss Prevention

College bookstore loss can result from shoplifting, internal theft, errors, or any combination of these. Studies show that literally billions of dollars are lost annually in college bookstores, and so it is highly advisable for bookstores to adopt retail industry loss prevention standards to benchmark effectiveness of any crime prevention programs that are put in place. Often, campus security is only brought into the bookstore for shoplifters, returned stolen goods, or possibly bank escort, however it is important for effective security management to apply retail shrinkage concepts in order to fully understand the potential magnitude of losses.

Shrinkage is the difference between the goods received and sold, and the goods in inventory, as a percentage of total sales. For example, a store received 250 shirts and sold 150, but inventoried only 90, meaning 10 shirts were missing. If the retail price of each shirt was $25, then a loss of $250 occurred. Since shirt sales totaled $3750, the shrinkage was 6.7% (250 divided by $3750). This is a theoretical example, but average retail shrinkage for 2002 falls at about 1.7%[4]. If a bookstore brought in $100,000 in sales, their loss would be $1850. This may not seem like a lot, but as a percentage of U.S. retailers sales amounts to more than motor vehicle theft, bank robbery, and household burglary combined. Often the difference between 1.5% and 3% is the difference between operating and bankruptcy.

[4] University of Florida Gainesville, Security Research Project, 2002 National Retail Security Survey

It is valuable for security management to look at these figures and understand also that statistically, retail security managers attribute employee theft with over 48% of losses, shoplifters with 32%, and the remainder to administrative errors or manipulation, and lastly vendors. They key four areas where retail focuses its attention for loss capture are:

- *Administrative offices*, where inventory, price, vendor, and accounting records are kept. These records are subject to manipulation and loss through theft or errors. False vendor files, faked deposit records, and improper inventory entries are a few examples. Loss prevention should include physical security (access control and/or CCTV), computer security, and checks and balances so no one person has complete control.
- *Cash Service Areas*, including the customer service desk, cash register stations, and cash counting/handling office. The customer service desk is especially a target for fraud since it handles customer returns and cash register operations. Shoplifting often occurs here with the unsuspecting cooperation of store employees. The thief will select an item from the clothing rack and bring it to customer service with the claim of returning it for being the wrong size. The thief gets the second item of clothing and brings it to customer service for bagging and removal from the store. The thief will sometimes demand a refund for the first item. Employees will sometimes work together for this type of fraud. Cash registers are subject to check and credit fraud, errors, under-ringing goods, and customer manipulation. Many of these cash service area losses can be greatly reduced with CCTV surveillance.
- *Customer venues,* including sales floor, fitting rooms, and rest rooms are often opportunities for shoplifters. Security patrols, cameras, security mirrors, locked display cases, and electronic inventory tags should be used as appropriate, however there is no substitute for good customer service as a deterrent to theft. It is worthwhile for Campus Safety to ensure bookstore employees are trained to deal with shoplifters when entering customer areas in order to prevent the crime before it occurs. Campus Safety should also be sure that bookstore employees are not incorrectly or inappropriately detaining a suspected shoplifter, so that litigation does not ensue from a false accusation. The use of force could also have disastrous results. Campus Safety can work with the bookstore to develop a training program so that bookstore employees clearly understand their legal limitations under probable cause, and when to summon Campus Safety for assistance.
- *Support locations,* such as employee break rooms, lockers, trash receptacles, storage closets, and shipping/receiving areas are especially high areas of internal theft. Routine inspection of lockers, storage areas, trash bins, and backpacks should be considered, and close management of the key control policy is mandatory. Shipping and receiving areas should be closely watched for employee theft as well as paperwork errors. Using physical security, process control, CCTV cameras, and alarm systems are all valuable measures to

use against loss. Shipping and receiving audit trails should also be used to ensure all items are correctly accounted for.

The bookstore at Chabot College is operated under the auspices of the College, rather than as an independent private business such as the bookstore on Las Positas campus. Based on the information developed in the site assessment, the Chabot bookstore is experiencing a level of theft that was also the case on Las Positas campus at one time. Las Positas and Follett Corporation have since taken specific measures to address theft such as employee training, additional CCTV, mirror surveillance, and an asset tracking system that have essentially solved the problems.

If the College decides to continue management of the bookstore at Chabot, there will need to be certain upgrades to the bookstore security program including ACAMS for door locking and increased CCTV surveillance in non-selling areas. CATALYST also recommends that the College consider installation of an asset tracking system such as the type in service at Las Positas which has proved to be very successful in catching shoplifters and deterring further crime. CATALYST further recommends that the College establish an employee training program to train employees in problem recognition and appropriate response methods that have proved instrumental in the success of the Las Positas theft prevention program.

Bookstore Video Surveillance - At Chabot College bookstore there is currently a CCTV system with fixed cameras and a video recorder that watches key areas of the store. This is an outdated VCR system that will not readily integrate with a new campus system. CATALYST recommends that along with the deployment of a new digital video recording on the campus, that the bookstore video system be upgraded to a digital video system that is compatible with the College system. The bookstore system should also be integrated into the College's main system, while still maintaining the bookstore as a viewing network client. This will allow Campus Safety to readily receive evidence video files from the bookstore for viewing, as well as respond to a request by the bookstore to assist in a surveillance effort.

CATALYST also recommends adding cameras to cover areas of the store where surveillance is not currently present, and theft is known or strongly suspected. This includes certain product isles where high value goods are located, non-selling areas such as hallways to break areas, the accounting room, and at the access doors to inventory storage.

Bookstore Access Control –Theft opportunity currently exists based on inadequate door locking capability within certain areas of the store. It is also possible for merchandise to move undetected into the break room or bathrooms for concealment or repositioning for later retrieval. Bookstore doors are

currently secured using key locks, however evidence has shown that keys are lost or not returned by former employees so that secure areas with key locking are compromised. According to the bookstore management employee turnover is high, which makes key control even more difficult. Greater security may be possible at least temporarily by re-keying the bookstore doors, although key management in the bookstore will continue to be challenging and costly. A better solution will be the application of access control on the critical doors leading to the accounting room, the break room area, and the main entry doors.

Specific to the theft crimes occurring in the bookstore, CATALYST makes the following recommendations for mitigation:

- Adopt a training program for employees to stress greeting the customer, being available to monitor customer actions, understanding how and when to detain a customer, recognizing suspicious behavior, and when to call in Campus Safety.
- Evaluate the causes for high employee turnover to at least reduce this effect and create a base of return employees.
- Restrict bathroom and break room use to employees only, and access-control the door leading into this area. Bathrooms are conveniently located outside the store for customers.
- Upgrade the CCTV recording system to be compatible with the College digital video system.
- Add cameras in those key areas not currently under surveillance where theft opportunity is available and surveillance by store employees is difficult or impossible.
- Add CCTV surveillance to observe the hallway leading to the break room area.
- Add concave mirror surveillance to assist the employees watching the store.
- If cash register theft is suspected, add POS cameras.
- Install Electronic Article Surveillance system (EAS) for detecting theft of key high value items.

9.5. Cash Handling

Cash is collected at a number of different locations on campus. During the site surveys and informal interviews, different cash handling procedures were discussed and concern was expressed over the current procedures and a recognized need for improvements. The time and days that the money is transported is fairly regular and the employees responsible for transporting the money are neither trained to handle potential robberies nor equipped to do so. While the loss of money to the District is a relatively minor risk, the potential political and legal impact that such a robbery could create is a much greater vulnerability.

CATALYST recommends the following guidelines for establishing a standardized Cash Handling Policy:

- Limit and secure access to any area where cash is collected, counted, and or reconciled.
- Duress alarms and CCTV cameras at desks where cash is handled, counted, and, or reconciled.
- Procurement and utilization of time-coded cash drop safes at locations where cash is collected.
- Limited access to the areas where the safes are located.
- Security alarms on the safes as well as within the rooms where the safes are located.
- Retention of an armored courier service to collect and deposit cash from the College, including random date and time of collection.
- Single point of accountability and responsibility within the District to ensure that the cash handling policies are followed and enforced.

10. Physical Security

10.1. Door Hardware

a. Locksets

Use only electro-mechanical locking hardware, 24 VDC, with request-to-exit devices incorporated into the hardware and fail-secure functionality. Use mortise lockset on all new doors, and whenever retrofitting to existing doors with mortise prep. Use Schlage "L" series locksets, or equivalent commercial heavy duty hardware. Do not use maglocks unless it is impossible to retrofit or replace the door for electro-mechanical hardware. Do not use door wire loops unless it is impossible to retrofit the door for wired hinges.

b. Exit Devices

Use only electro-mechanical locking hardware, 24 VDC, with request-to-exit devices incorporated into the hardware and fail-secure functionality. Use mortise, rim, or dual-rod devices as appropriate for the opening design of single or sets of double doors. Use Von Duprin "98/99" series, or equivalent commercial heavy duty hardware. Do not use maglocks or "touch-sense" bars unless it is impossible to retrofit or replace the door for electro-mechanical hardware. Do not use door wire loops unless it is impossible to retrofit the door for power transfer devices or wired hinges

10.2. Access Control and Alarm Monitoring Systems (ACAMS) - Applications

Application of ACAMS will be presented for two basic conditions, renovation of existing buildings and construction of new buildings.

a. Existing Building Renovation

The Chabot College buildings are typically one primary design with a limited number of outside main entrances to each building, and interior access to classrooms and labs from corridors. Some of the buildings on District campuses are currently equipped with burglar alarm or Sonitrol systems. These burglar alarm systems are from various different manufacturers, and are currently all being monitored by third party alarm monitoring companies. There are also some service buildings and the athletic buildings which have main entrances directly from the outside.

With this in mind, the following section details CATALYST's security recommendations for existing building renovation projects keeping in mind renovations are solely referring to security renovations as opposed to architectural renovations.

ACAMS Recommendations

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 any existing alarm system keypads with card reader/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. Utilize door hardware that incorporates request-to-exit devices within the hardware whenever functionality and design permit.
F. Provide door alarm contacts on all perimeter and service doors that are not card reader controlled entrance points.
G. Install access-controlled doors with card readers to secure all telecommunication/data rooms.
H. 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 such as Audio-Visual, diagnostic or electronic equipment, theatre arts, musical equipment, retail items, etc.
    c. Potentially dangerous equipment.
    d. Hazardous equipment.
    e. Items that present an attractive nuisance.

f. Laboratory equipment and chemicals.

(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.)

I. Install access-controlled doors with card readers to 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 College or 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.)

J. Provide alarm notification devices (robbery/duress buttons) at locations where money is handled, counseling offices, and high profile administrative offices.

K. Provide Cyber locks on doors where criteria are not sufficient to justify incorporation of card readers at this time, but where a level of security is desired greater than mechanical keys will provide. Cyber locks may be used as a carry-over security measure for a building access that needs to be secured at this time, but is scheduled for renovation or new construction and will ultimately be incorporated into the ACAMS.

L. Equip all building perimeter doors not already fitted with access control with door contacts that are terminated to the building ACAMS panel and programmed as alarm points.

M. Equip all gates that contain child recreation areas with gate alarm contacts, terminated to the ACAMS and programmed as alarm points. Install local audible alarm sounders in the near vicinity of the gates that are powered ant triggered through the ACAMS on a gate opening event.

b. New Building Construction

New building construction provides an excellent opportunity for the implementation of campus security systems. The ACAMS will provide a more secure environment for employees, students and visitors, 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. With this in mind, the following section details CATALYST's recommendations for security criteria for new building projects.

ACAMS Recommendations

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. Utilize door hardware with built-in request-to-exit devices wherever functionality and design permit.

D. Provide door alarm contacts on all perimeter and service doors that are not card reader controlled entrance points.

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:

    1. Cash.
    2. Equipment of high dollar value such as Audio-Visual, diagnostic, theatre arts, musical equipment, retail items, etc.
    3. Potentially dangerous equipment.
    4. Hazardous equipment.
    5. Items that present an attractive nuisance.
    6. Laboratory equipment and chemicals.

    (Note: Internal areas that will also be 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.)

G. Install access-controlled doors with card readers to 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 will require a card reader/keypad for internal alarm arming and disarming functionality.)

H. Provide alarm notification devices (robbery/duress buttons) at locations where money is handled, counseling offices, and high profile administrative offices.

I. 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 such as Audio-Visual, diagnostic, theatre arts, musical equipment, retail items, etc.
    3. Potentially dangerous equipment.
    4. Hazardous equipment.
    5. Items that present an attractive nuisance.
    6. Laboratory equipment and chemicals.
    7. Campus computer network equipment and infrastructure.
    8. Sensitive information that could be potentially damaging to the College or District if made public.

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

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

K. Provide Cyber locks on doors where criteria are not sufficient to justify incorporation of card readers at this time, but where a level of security is desired greater than mechanical keys will provide. Cyber locks may be used as a carry-over security measure for a building access that needs to be secured at this time, but is scheduled for renovation or new construction and will ultimately be incorporated into the ACAMS.

L. Equip all gates that contain child recreation areas with gate alarm contacts, terminated to the ACAMS and programmed as alarm points. Install local audible alarm sounders in the near vicinity of the gates that are powered ant triggered through the ACAMS on a gate opening event.

c. Access Control and Alarm Monitoring System (ACAMS) Control Hardware

ACAMS control hardware is required to operate the systems and devices as described above. Typically, the ACAMS throughout the Campus will operate of a single, centrally located ACAMS server and the individual devices will be controlled ACAMS control panels and power supplies located in each building where the devises are installed. The following details the requirements for the ACAMS control equipment.

A. ACAMS Server - Locate ACAMS server in a secured, access-controlled room, typically a telecom or data closet or MDF room. Servers should be sized for no less than 25% excess capacity of transaction memory and card holder database.

B. ACAMS Control Panels - Locate ACAMS control panels in a secured, access-controlled room, typically a telecom or data closet or MDF room. ACAMS control panels must be in an enclosed locked cabinet, fitted with a tamper alarm.
C. UPS – Provide each server with a dedicated UL Listed UPS capable of no less than 1 hour of back up power in the event of a power failure.
D. Lock Power Supplies - Use only UL Listed power supplies, 24 VDC, Located in near proximity to ACAMS control panels in a secured, access-controlled room, typically a telecom or data closet or MDF room. Power supplies must be in an enclosed locked cabinet, fitted with a tamper alarm.

10.3. Closed Circuit Television System (CCTV)

CCTV systems help to supplement the ACAMS to provide a comprehensive approach to security. CCTV can extend the Campus coverage and response without adding additional staff. Recent enhancements in technology have revolutionized the CCTV industry with the advent of digital video recorders, network compatibility, ultra low light sensitive cameras and direct integration with other security equipment.

The goals of CCTV surveillance will be to obtain usable video evidence that can be part of post-incident investigation, as well as provide some level of active monitoring in selected crime prone locations as a risk reduction measure. The video quality has to be sufficient to reproduce identifiable characteristics of individuals and actions or items involved in a security or safety event, so available lighting and camera types must be factored for the best results. Video Monitoring will be managed by the Campus Safety department.

Understanding that the college environment is not conducive to widespread CCTV coverage, strategic locations where cameras will assist in the safety and protection of the employees, students, and visitors are recommended. CATALYST recommends that cameras be positioned to view specific locations such as building entry points, parking lot entry/exit points, high value storage areas, key sports facilities, areas of high potential loss due to theft or vandalism, and cash handling or retail areas.

CATALYST recommends that the College install a CCTV system incorporating digital recording technology, which will provide a PC-based solution to the end-user. The DVR solution will provide the following features:

- Pre- and post-alarm recording of security events, which allows the viewer to see what happened before and after an alarmed event.
- Recording frame rate increase upon alarm event.

- Adjustable recording frame rates on a per camera basis.
- PC hard drive storage technology.
- Incorporation of CCTV inputs and control.
- Built-in Ethernet network compatibility, which allows for centralized storage of video archived from multiple sites.

CCTV Site Recommendations

A. Install CCTV DVR's in the each building that contains video surveillance cameras. Typically, the CCTV digital video recorders/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 internal areas that house any of the following physical items with high resolution color
C. CCTV cameras:
    a. Cash.
    b. Equipment of high dollar value such as Audio-Visual, diagnostic, theatre arts, musical equipment, retail items, etc.
    c. Potentially dangerous equipment.
D. Equip internal areas where cash and/or records transactions occur with high-resolution CCTV cameras to view and record interactions.
E. Equip major building entrances with high-resolution color CCTV cameras.

In conjunction with the distributed DVR equipment, CATALYST recommends that the College install high resolution, low light, color CCD fixed and pan-tilt-zoom cameras at strategic locations throughout the campus. Finally, the digital video system should be integrated with the ACAMS to provide alarm call-up of specified cameras in the security control center during alarm conditions.

10.4. Security Communications Systems (SCS)

As presented previously in the Vulnerability Analysis, there is currently a need to improve the capability for emergency communications in the instructional buildings as well as other key areas on campus. The instructional buildings need a readily accessible voice communications system that could contact emergency services through campus safety as well as provide normal voice communications within the campus. This would typically be a telephone system installed in the classrooms where possible.

There are also locations on campus where the installation of duress buttons is highly advisable, due to the nature of the threat potential at these locations. These locations are listed below as part of the total overview of the Security Communications System, along with the relevant recommendations for those areas:

- Instructional buildings and classrooms
    - Install telephones or emergency voice devices in classrooms where possible and in building hallways where it is not possible.
- Any locations where cash is handled
    - Install duress buttons.
- Administrative, financial aid, and registration offices
    - Install duress buttons at locations where potentially threatening situations exist.
- Counseling offices
    - Install duress buttons and telephones or emergency voice devices
- Health Services
    - Install duress buttons and telephones or emergency voice devices
- Child Day Care
    - Install duress buttons and telephones or emergency voice devices
- Public areas and parking lots
    - Expand the coverage of telephones or emergency voice devices

CATALYST recognizes that simply installing these devices do not ensure their effective or proper use, and that the need for usage training is vital to the success of using these types of systems as well as the personal safety of the users who intend to depend on them. This is especially true for the duress buttons, since activation is intended to indicate a duress condition of relatively serious nature. As part of the deployment of the duress and emergency communications systems, CATALYST recommends that instructional training be developed through Campus Safety and presented to the user groups on an introductory and refresher basis.

Security communications also includes the parking lot and campus "blue-light" emergency call stations, the Campus Safety MRTI (Microprocessor Radio Telephone Interface) system, and the conceptual site all-call system.

Emergency "blue-light" call stations located in the parking lots and at various campus locations are used regularly by the campus population to request assistance, indicating that the students and staff have become comfortable and familiar with their use. While the current system provides definite security benefit of some emergency communication capability and a sense of security for the more remote areas of the campus, the system is half-duplex one-way communication, it does not have a method of indicating the location of the caller, and the location indicating blue lights on the boxes are low power making them difficult to see at night. There also are not enough of the call boxes, especially in the parking lots and outlying areas of the campus. CATALYST recommends upgrading

the emergency blue-light call stations to a system with full-duplex communication. This will allow "telephone-like" conversation between Campus Safety and the caller. This will also allow Campus Safety to hear noise or voices in the background of a caller, should they be in distress and not be able to verbalize their problem. The upgraded system should also have a method of indicating the location of the calling station in plain English, and have a sufficiently bright set of beacon and strobe lights to call attention to their location day or night. The density of the emergency call stations also needs to be increased to add more stations in the parking lots in order to reduce the distance between stations to approximately 300 feet max. Additional pole type stations need to be located around the campus, exterior to the instructional and administration buildings, on the pathways and in clear view.

MRTI is a Motorola based system that was installed at the College in the mid-1990's as a method to interconnect radio communication with telephone communication. This system currently offers Campus Safety numerous benefits of having one roving guard be able to field telephone calls as the predominant mode of communication from sources outside of the Campus Safety Department. The challenge with this system is that it is dated by today's radio, telephone, and cell communication standards, and based on CATALYST's research will be difficult to support in the near future. Motorola has stopped manufacturing this system and considers it obsolete; parts that are available are within the network of dealers that have inventory of this system. Although further research will be required to determine the range of replacement options and their relative impact, Motorola is branding a replacement system for TI (Telephone Interface) applications, manufactured by Zetron. For example and discussion sake, the Zetron specification sheet is attached as Appendix C.

There is currently no method of readily dispatching emergency notification information such as "Evacuation" or "Shelter in Place" to the entire campus simultaneously. Historically this type of information has been passed by word of mouth via "runner", or possibly though an inter-campus telephone system. As mentioned previously, there is not a telephone system throughout the campus that can accomplish this type of communications, so currently this notification if needed, would be done by word of mouth. Technology is available that can incorporate site "All-Call" functionality into many of the newer fire detection and alarm systems. CATALYST understands that Chabot is currently mid-phase in a 5 year renovation plan for their existing Simplex fire system. Whether the new system can have this functionality or not is indeterminate at this time without further research, however CATALYST recommends that All-Call capability be incorporated into the security control room, whether it is a feature of the fire system or another separate announcement system. CATALYST is continuing to research the capabilities of the system being installed currently, and will present the options to the College when the information becomes available.

10.5. System Integration

System integration was mentioned in the CCTV section, stating that the CCTV system needs to be selected and designed for compatibility and integration capability with the ACAMS. This concept of inter-system compatibility needs to also apply to most other systems that are deployed within the operating responsibility of Campus Safety. Similar to the positive aspects of how a suite of office software has interrelationships that make for a more powerful total program, likewise fully compatible security systems with the capability for close system integration can bring the operation of diverse systems successfully and seamlessly to a single point. The operator can have the capability from one point to control alarm monitoring, CCTV, access control, digital video recording, badging, intercom, visitor management, email, paging, and many other functions when the system integration is planned correctly. This concept of close integration is especially important when the District considers a single security control center for both Chabot and Las Positas Colleges. From the IT manager's point of view, a single software suite that meets the District network requirements is also an advantage, since licensing and software maintenance become greatly simplified.

At the center of the system integration selection is the access control system. This is the key software package and main server that will need to be compatible with all other campus systems. It is CATALYST's recommendation that as a baseline set of standards, the selected access control system have the following minimum features:

- Microsoft Windows 2003/XP based
- Open Architecture design
- Client/Server Architecture
- Custom Report Capabilities
- Alarm Monitoring
- CCTV and Digital Video Integration
- Database Partitioning
- Mustering
- Email and Paging
- ODBC Compliancy
- Distributed Network Capability
- Visitor Management
- Mobile Client Capability

The District has not engaged CATALYST at this time to develop the methodology or product demonstration schedule to facilitate selection of the security management software. CATALYST

recommends that a program is defined for the review of product alternatives and selection of system head-end software.

10.6. Security Electrical and Network Requirements

Cable: Cabling Methods for security systems will follow standard electrical practices used in the building construction or renovation. Wire and cable specifications will be addressed in the construction documents and describe wire pulling, cableways, grounding, and termination methods. ACAMS control panels will be connected to and configured on a secure VLAN across the District Ethernet LAN. Cabling will be CAT-6, and in accordance with current LPCCD standards for the College site. Cabling for the video system will use fiber, unshielded-twisted pairs (UTP), or coax as needed in the specifically designed location. Video DVR's will also communicate inter-campus via the secure VLAN. To provide video capability to both Chabot and Las Positas campuses within the security control center, video DVR's will communicate across the District Ethernet LAN.

Network Distribution: At the time of the security survey, a survey was being conducted simultaneously to assess the quantity and viability of the existing site fiber and cable. CATALYST understands that the results of this survey information will be made available for the design process to determine if new or existing infrastructure will be utilized.

Based on the assessment of the main network room distribution layout, most of the campus is currently being served by fiber a communication backbone, with some amount of spare capacity to certain buildings. The one building that does not currently have adequate fiber or CAT-5/6 service is Building 1300. CATALYST has recommended that some security devices (ACAMS and cameras) be installed in the theater area to reduce the current theft and vandalism risks. This will require that additional fiber and CAT-5/6 communication be supplied to building 1300, in addition to any other buildings which will be determined at the time of design.

Intermediate Network: During the security survey, CATALYST also evaluated the condition, locations, and availability of the network distribution closets. Most of the intermediate distribution points have been located in janitor's closets due to need for available space and convenience. The janitor's closet spaces are problematic due to frequent access by campus personnel who are not authorized to have access to network infrastructure. The equipment is also not installed within enclosures or locked.

Without the equipment in a locked, protected enclosure, it can easily be tampered with or accidentally damaged. The equipment is also typically placed in a high location in the closet, making it difficult to perform normal service. Ideally, any network distribution points should be within their own dedicated

closets, and access-controlled for entry only by authorized personnel. If it is not feasible or possible to build out separate network/telecom closets in every location, CATALYST recommends that at least in the locations where space must be shared, the network equipment is installed in an enclosed, locked metal cabinet designed for network and telecommunications equipment.

Main Network: The main network distribution room is currently located in a space that is scheduled for renovation as part of the IT offices and control center. While it has been set up to best utilize the available space, and the network was installed with some spare capacity to serve most of the campus, there are cable management and equipment set up problems that should be corrected at the time of renovation. The racks and panels are too close together for convenient servicing, not allowing sufficient space to walk or stand behind the racks and in front of the panels.

Cable and fiber that runs into the room is mostly bundled and routed correctly, however the current state of cable management from approximately the ladder level down does not make it possible for standard cabling and troubleshooting methods to be applied.

CATALYST recommends that during the renovation, this area of cable and fiber needs to be re-installed using standardized cable management methods for routing, bundling, labeling, and terminating. Additionally there is a considerable amount of stored materials in the network room that does not allow for clear walking paths and work areas. All excess and spare material should be removed from the network rooms, so that these rooms may be more easily maintained and are only accessed for the business of network management.

10.7. Parking Lot Security

Auto thefts from the parking lots at Chabot College are one of the key problems for Campus Safety and Security. The factors contributing to this are access opportunity to the vehicles and lack of visibility of the crime taking place. The opportunity is provided by open access and egress through all parking lots, which allows the criminal to take the target vehicle from the lot without any delay. Parking lot entry is open to the public and rapid exit capability makes detection more difficult. This condition is compounded in the evening with areas of low lighting. CATALYST has recommended increases in lighting in following sections of the Master Plan, and one of the key methods to reduce the opportunity factor is controlling the vehicles into and out of the lots. The College has also requested the installation of video surveillance for the parking lots, and CATALYST concurs that this is a worthwhile and feasible risk reduction measure.

Currently the normal parking lot use by students or employees is through purchasing a semester pass or daily ticket from lot vending machines. This process works to a certain extent, but also requires

consistent management by Campus Safety and regular maintenance by M&O. CATALYST has recommended that ACAMS be deployed on the Chabot campus, which if utilized can also be used to reduce the issuance of parking passes, and at the same time improve the control of vehicles in the lots. CATALYST also anticipates that the renovation and redesign scheduled for the parking layout will include some measure of vehicle speed and flow control that can be incorporated into the security improvement measures.

From the population of parking lot users some amount are campus employees, who will already be assigned an access control badge with the ACAMS. Likewise, some amount of parking lot users are students who purchase long-term or semester passes for parking. Sufficient parking space for these two groups should be allocated in staff or public lots as necessary. In addition to the student parking passes, CATALYST recommends that the student group of parking users also be issued an access control credential that can be used with the ACAMS and a card reader. The parking areas allocated to accommodate this population of employee and student users can then be managed by standard vehicle control methods such as barrier arms using a card reader to enter and free exit. Depending on the size of the student user group will determine how much of the parking areas can now be access controlled, and the amount of reduction to the available opportunity for free access to target autos. The reduction of free access parking will also allow Campus Safety to reduce the high problem parking zones to a smaller area.

In order to accomplish access control in the parking lots CATALYST recommends the following measures be applied:

<u>Parking Lot ACAMS</u>

A. Install ACAMS control panels with communication to ACAMS server in order to serve as interface for access control and alarm monitoring devices in new and existing parking lots. Typically, the ACAMS controllers will be installed in a secure room within a building nearest to the parking lot being served, and will be connected to and configured on a secure VLAN across the District Ethernet LAN.
B. Plan for ACAMS and barrier arm operation at main entrances to at least the staff parking areas, with infrastructure electrical paths for expanding the system to adjacent lots if the College desires the additional parking control.
C. Equip exits with automatic exit only barrier arms and/or grilles.
D. Equip vehicle exit paths with speed control bumps and lane separation islands for defining entry and exit travel paths.

Parking Lot CCTV

A. Install CCTV DVR's in a secure room within a secure room in a building nearest to the parking lot being served. The DVR will be connected to and configured on a secure VLAN across the District Ethernet LAN.
B. Install high-resolution color CCTV cameras to view the entrance and exit lanes of the lot.
C. Install high-resolution color CCTV cameras to provide general surveillance viewing down the parking lanes and ticket vending stations.
D. Install high-resolution color CCTV cameras in parking lots to view the Security Communication Stations discussed below.

Parking Lot Security Communications Systems (SCS)

A. Upgrade the existing emergency call stations to a system with two-way, full duplex communication capability.
B. Install freestanding bollard style call stations in parking lots at approximately 300' intervals. Size, location and use specific parking lots will determine the specific quantity and placement of the call stations.
C. Use call stations with bright locator always on blue beacon, and call-indicating high intensity blue strobe.
D. Terminate call stations to the College phone switch and program to automatically dial the security control center.

10.8. Fencing

Although numerous studies and testing have proven that fencing does little to prevent a determined criminal from entering the premises, it does provide a defined barrier from the casual trespasser and will delay or deter most attempts to enter. For the College, it also separates their property from the street and residential neighbors to the north and west. This is a reasonable area to install fencing, since it is the most remote area of the campus, and therefore the most difficult to patrol and protect. It is arguable that some level of fencing around the perimeter to enclose the street sides of the parking lots would provide a large measure of risk reduction for auto theft, vandalism, and auto burglary; however it may not be acceptable or feasible to fence this amount of the campus. Since there is currently fencing is in place in certain areas, it needs to be maintained in a straight condition, with gates operating normally and in parallel.

CATALYST found that some of the fencing along the west border is in excellent condition, while most of the north border fencing is in need of repair. This is especially the case for the gates in the northwest, and the gates leading to "J" parking. With properly installed top and bottom rails, fence testing has proven is that fence height is the most important factor in preventing jump-over. The fence

height along the north border is an acceptable height, however the fence fabric, and barbed wire top are in need of repair or replacement. Fence height is brought up since the gates at the northwest have clearly been jump many times over the years. CATALYST recommends that these gates be rebuilt to a new height of not less than 8 feet. This height increase should also carry over to the apron fencing leading to the gates that is accessible from the public street. Likewise the gate leading to "J" parking is bent and gapped possibly from vehicle impact, and there is no barbed wire top on the entire section that is common with the parking lot. CATALYST recommends that the gate be repaired or replaced to original standard, and basic pipe bollards be installed in front of the gate to protect from vehicles.

Summary of fencing recommendations:

1. Repair fencing along the entire north boundary to original standard. Angle top barbed wire rail 45° outward to deter jump over from outside College property.
2. Replace northwest gates. Install new gates of not less than 8 feet total height, including barbed wire top.
3. Increase fence height of apron on either side of northwest gates to match new 8 foot height of gate.
4. Repair or replace gates leading into "J" parking lot to restore original standard.
5. Install 3 removable, locked pipe bollards in front of the "J" gates, on the parking lot side.

10.9. Lighting and Landscaping

It is recommended that Chabot College lighting be designed to incorporate general principals of Security Lighting, as follows:

- Integrate light into the total security system and thereby facilitate the effectiveness of other security devices or procedures.[4]
- Illuminate objects, people, and places to allow observation and identification and thereby physically reduce criminal concealment.[4]
- Use illumination to deter criminal acts by creating a fear of detection, identification, and apprehension.[4]
- Reduce the fear of crime for the innocent by enhancing a perception of security.[5]
- Security lighting is an essential and fundamental element in a well-established physical security program.
- Security lighting will serve as a deterrent to potential violators.
- Security lighting assists security personnel for identification purposes.
- According to a National Institute of Justice (NIJ) Research Brief, published in April 1996, lighting is one of the few facility features that have been documented to reduce crime.

[4] IESNA LIGHTING HANDBOOK, Ninth Edition (2000).

Security Lighting Standards. There is no current U.S. 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. The standard has since been withdrawn and no formally adopted standard has been issued.

Although there is no current U.S. national standard for protective or security lighting, the Illuminating Engineering Society of North America (IESNA) is the recognized technical authority on illumination. Through its technical committees, the IESNA publishes recommended practices regarding lighting applications such as security lighting. The IESNA design guidelines are the most recognized reference for Security Lighting.

Factors which affect Security Lighting:

- Crime status of the area.
- Nature of the site: The campus is in a rural area, surrounding area is open grassland. The campus will be an open campus (not enclosed or controlled), accessible all hours, all days of the year.
- Degree of obstruction: Potential obstruction of light due to landscape design and building configurations.
- Ambient brightness of the surrounding area: This factor actually has a negative impact on the campus lighting criteria, as there is no neighboring or surrounding areas with at light source.

Recommended Average Illuminances 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 illuminance values are listed, other values such as vertical illuminance and determination of light characteristics, i.e., color appearance, glare, shadows, etc., will be interpreted and applied by the lighting designer. For purposes of this document and IESNA illuminance values, the campus was considered a "Controlled Site". The campus also has areas which can be considered "Public Spaces" because it is an open campus to which there is unrestricted public access. In the table below, abbreviations "lx" is lux and "fc" is foot-candle.

IESNA – Recommended Lighting Levels

Illuminance:	Lux (lx)	Foot-candle fc)	See Note 1
Large Open Areas:	5 to 20	0.5 to 2	See Note 2
Building Entrances:			
Active (pedestrian/conveyance)	50	5	
Inactive (normally locked, infrequent use)	30	3	
Parking Lots	10 to 50	1.0 to 5	See Note 3
Covered Parking Facilities	60	6	

Parks, Plazas, and Pedestrian Malls	50	5
Sidewalks and Footpaths, and	6	0.6
Grounds Around Open Parking Lots	6	0.6
Trails and Walkways	6	0.6
Areas Around Open Parking Lots	6	0.6

Notes:

1. A foot-candle 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.

Other Documented Lighting Standards:

Department of Army, Field Manual 3-19-30 recommends the following values:

0.2 fc Outer perimeter
0.4 fc Restricted area perimeter
1.0 fc Vehicular entrances
2.0 fc Pedestrian entrances
0.2 fc Sensitive inner areas
1.0 fc Sensitive inner structure
2.0 fc Open yards
1.0 fc Decks on open piers

Architectural Graphic Standards recommends the following:

	Commercial	Intermediate	Residential (in Foot Candles)
Pedestrian Areas:			
Sidewalks	0.9	0.6	0.2
Pedestrian ways	2.0	1.0	0.5
Vehicular Roads:			
Freeway	0.6	0.6	0.6
Major road & Expressway	2.0	1.4	1.0
Collector road	1.2	0.9	0.6
Local road	0.9	0.6	0.4
Alleys	0.6	0.4	0.2
Parking Areas:			
Self-parking	1.0	-	-
Attendant parking	2.0	-	-
Security problem area (high crime)	-	-	5.0

Minimum for television viewing of important interdiction areas	10.0	10.0	10.0
Building Areas:			
Entrances	5.0	-	-
General grounds	1.0	-	-

Chabot College Lighting Survey:

CATALYST performed night lighting surveys to identify whether or not lighting was acceptable in parking lots and along normal paths of travel, based on IESNA and AIA standards. CATALYST evaluated the security lighting, also considering ambient brightness of the surrounding areas, obstructions from buildings, and landscape design. In recent years, the College has installed some lighting upgrades to selected dark areas of the campus, especially the parking lots. Although the lighting upgrades have definitely improved visibility on some parking areas, CATALYST's night survey found that numerous travel paths still have low or non-existent lighting. The problem areas where lower than standard lighted was measured are divided into two sections, Perimeter and Grounds, and Campus Interior. The following is a list of the general areas of low light measurement:

Perimeter and Grounds:

1. The southeast sides and corners of Parking Lot G, along Hesperian Blvd. and Depot Road.
2. The Depot Rd. entry of Parking Lot G.
3. The Depot Rd. Entry of Student Parking Lots F and E.
4. The perimeter border of Lots C, D, and E along the western access road.
5. Parking Lot D – No lights at all.
6. The entire athletic field.
7. The northern border of Parking Lot B
8. The entry road and foot paths from Hesperian Blvd. To Parking lot B.
9. The bus stop shelter and most of the sidewalk area surrounding the shelter.
10. The western sidewalk between the bus stop exit and the entry to Parking Lot G.
11. The entry road and foot paths from Hesperian Blvd. To Parking lot G.
12. All the large grass and tree areas on the west side of the campus and along Hesperian Blvd.
13. Parking lot locations greater than ~ 100 ft from a main light pole.

Campus Interior:

1. Walkways radiating out from the oval courtyard covered walkway.
2. Walking area on the back side (field side) of Bldg. 2900.
3. Walk path from parking toward pool complex entry at Bldg. 3200.

Recommendations for Lighting.

The measures to correct areas of low lighting should first be directed to those locations that correspond to the areas of high crime risk. CATALYST recommends addressing security lighting improvements in the following order:

- The first priority is the parking lots. Clearly Parking Lot "D" which has no lighting, and the perimeters of Parking Lots B, G, F, and E that border the city surface streets and have very little lighting are the locations that need attention first.
- The second priority level for upgraded lighting is also parking lots, but focusing on the overall general lighting of the two main lots G and B. Using the same type of fixture, increase the number of fixtures per square area.
- The third priority is lighting between campus buildings. Lighting between buildings needs to be raised to minimum illuminations standards.

Landscaping

Since landscaping directly correlates to lighting effectiveness, CATALYST also evaluated any landscaping interferences with lighting or normal viewing ability. A key theory of Crime Prevention Through Environmental Design[6] (CPTED) is "natural surveillance". This is a design concept, using natural features to enable one's ability to view the space around them, maximize visibility, increase one's awareness, and thereby reduce the vulnerability for crime. Landscaping, 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.

As a related recommendation for landscaping, shrubs should be maintained below 3 feet, and trees should be trimmed up 7-8 feet. Lacey trees are more appropriate for visibility. CATALYST found the landscaping on Chabot College campus to be very well maintained, and for the most part aimed at achieving the intent of this security standard. Almost all trees are trimmed up 7-8 feet and shrubbery is kept low. There were only a small number of locations that CATALYST found where landscaping is overgrown or incorrect for security standards. The locations are:

- Around the main entrances to some of the campus buildings, landscaping shrubbery is growing high enough to provide hiding areas. This is especially a concern due to their proximity to the building entrance. The most noticeable locations were at the entrance to Building 700, and the area behind the patio of Building 3500.

---

[5] Timothy Crowe, Crime Prevention Through Environmental Design, Second Edition, (Butterworth Heineman, 2000)

- Vine ivy growing in the islands and borders of the parking lots is high and deep enough to provide hiding areas. This is a concern due to the close proximity to people parking their cars. The most noticeable area is the sides of Parking Lot "B" entry from Hesperian Blvd and the Parking Lot "B" border with Hesperian Blvd.

The recommendations for these areas are to reduce the landscaping height and density.

11. Conclusion

Chabot College and the District have an unprecedented opportunity to bring their institution up to a modern standard for safety and security. The site survey did not find glaring problems or an excessively dangerous environment; however there is a distinct incident rate of certain Part 1 and Part 2 Offenses. If the College and District elect to implement the SMP recommendations, significant improvements in mitigating campus crimes of auto theft, petty theft, auto burglary, and vandalism will be realized providing consistency is maintained in the approach to applying the new security measures. Campus Safety will always need to remain diligent to the influences of certain crimes from the surrounding community; however the security measures in this SMP will provide the officers, Security Director, and campus administrators with a solid base of crime prevention and risk reduction strategies to support their efforts. It should be reiterated that all new systems and features on the daily landscape mean a change of some level, and the recommended changes of access control, CCTV, communications, and processes will affect the campus population. A brief summary of the recommendations detailed within the report are included here for review.

- Upgrade the Parking Lot Lighting to at least minimum IESNA standards.
- Install CCTV cameras to view designated areas of the parking lots.
- Install a digital video recording solution for capturing the CCTV information. Ensure that the system will have the capability for integration as detailed in the SMP.
- Select and deploy the ACAMS to the campus buildings, beginning with integration of the existing alarm monitoring system and installation of duress buttons in high risk areas.
- Begin upgrading staff parking lots to ACAMS in conjunction with architectural plans for parking lot modifications.
- Upgrade Security Communications Systems, beginning with high incident parking lot areas, and continue by increasing the distribution density of the emergency call stations throughout all parking lots and the main campus.
- Bring other parking lots on the ACAMS as modifications, badge deployment, and funding allow.
- Establish campus location and construct District Security Control Center at Chabot College.

Appendix A

Crime Statistics

- *CRIMECAST*® Standard Report
- *CRIMECAST*® Site Report
- UCR California Crimes by County, 2003
- UCR Alameda County Crimes, 2003 per 100,000 population
- UCR Alameda County Crimes, 2002-2003
- Chabot College Department of Campus Safety, 2004 Crime Statistics

Appendix B – Glossary of Terms

ACAMS	Access Control and Alarm Monitoring System
ADA	American's with Disabilities Act
Badge	Electronically enhanced plastic card for identification, system activation, and database interface.
CCD	Charge Coupled Device
CATALYST	CATALYST Consulting Group
CCTV	Closed Circuit Television
CSO	Community Service Officer
Campus Safety	Chabot Community College Office of Safety and Security
District	Chabot Las Positas Community College District
DVR	Digital Video Recorder
MRTI	Microprocessor Radio-Telephone Interface
SCC	Security Control Center
SCS	Security Communications System
SMP	Security Master Plan

Appendix C

Zetron Mobile Radio Telephone Interface – 48*jr*

Appendix D
Security Field Device Matrix