SECURITY MASTER PLAN OUTLINE

for

CHABOT LAS POSITAS
Community College District

Submitted by:

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

May 2, 2005
SECURITY MASTER PLAN OUTLINE

Chabot
Community College District

This outline presents the fundamental topics of the Security Master Plan, an independent document incorporated by reference into the TBP Architecture District Master Plan for the Chabot College campus new construction and building improvements. 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 Security Master Plan will include the topic sections listed in the outline following.

The primary intent of the Security Master Plan is to define security mitigation standards that integrate efficiently with new building construction and building improvements, saving upgrade costs today by planning for the campus of tomorrow. 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, CATALYST will present a clear security philosophy to guide the selection and implementation of campus security upgrades. The Security Master Plan will be developed to address long-term system compatibility, communication infrastructure, product obsolescence, and growing demands on the security staff.
Outline of Topics for Security Master Plan

I. Executive Summary

II. Introduction

   A. District Goals and Objectives
   B. Statement of Scope
   C. Description of Process and Implementation (see Appendix A)
   D. Risk Analysis Review
      a. Asset Definition
      b. Threat Assessment – Prior, Existing, Future
      c. Vulnerability Analysis
   E. Loss Prevention Recommendations
      a. Criticality Cost Factors
      b. Loss Total Costs
      c. Loss Avoidance, Transference, Mitigation

III. Security Program Recommendations

   A. Management and Administration
      a. System Life-Cycle Ownership
      b. Daily Operations
      c. Database and Server Management
   B. Security Staffing, Supervision, and Training
   C. Control Center
      a. Operational Requirements
      b. Technology Requirements
      c. Communications
   D. Security Awareness Training
      a. Student Orientation
      b. Ongoing Training
   E. Crisis Response and Recovery Plans
      a. Public Service Liaison
      b. Drill Planning

IV. Operational Policies and Procedures

   A. Identification and Badging
      a. Badge Issuing
      b. Badging Systems Management
   B. Card Access Control (ACAMS)
      a. ACAMS Applications at Entry Points
         i. Exterior Building and Departmental Control
         ii. Interior Critical Areas
      b. ACAMS Data Management
C. Visitor Access Control
   a. Invitee Access Control
   b. Vendor and Contractor Access Control

D. Key Control
   a. Key Control Policy
   b. Key System Manager

E. Theft and Loss Prevention
   a. Bookstore Shrinkage and Benchmarking
   b. Library
   c. Shipping & Receiving

F. Incident Reporting
   a. Reporting Methods and Facilitation
   b. Response Mechanism

G. Cash Handling

V. Physical Security Recommendations

A. Door Locking Hardware
   a. Locksets
   b. Exit Devices

B. Access Control and Alarm Monitoring System (ACAMS) Hardware
   a. ACAMS Servers
   b. Intelligent Field Panels
   c. UPS
   d. Electronic Locking Devices
   e. Lock Power Supplies

C. Access Control and Alarm Monitoring (ACAMS) Software
   a. Software Administration
   b. Report Generation

D. Access Control and Alarm Monitoring Field Devices
   a. Perimeter Door Alarms
   b. ACAMS Event Reporting Devices
   c. System Remote Communications

E. Identification and Badging System
   a. System Deployment
   b. Badge Control
   c. Life-Cycle Badge System Management

F. Closed Circuit Television Monitoring and Recording
   a. Goals of CCTV Surveillance
   b. Video Monitoring

G. Exterior Area Intrusion Detection

H. Security System Integration
I. Electrical and Architectural Requirements  
   a. Cabling Methods  
   b. Secured Equipment Locations  

J. Network Clients  
   a. Authorization of Clients  
   b. Network Connectivity  
   c. Client Service Level  

VI. Physical Security Applications  

   A. External Barriers (Fences, Gates, Etc.)  
      a. Perimeter Control  
      b. Interior Barriers  

   B. Exterior Area Protection  

   C. Exterior Security Lighting  
      a. Parking Areas  
      b. Pathways  
      c. Campus Buildings  

   D. Employee/Visitor Parking Areas  
      a. Access and Egress  
      b. Adjacent Surface Street Parking  

VII. Site Specific Recommendations  

   A. Chabot College
APPENDIX A.

Overview of Process and Implementation Methods

A. Purpose and Process of the Site Surveys and Interviews

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 actually 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, CCG’s objective was to gather perceptions of vulnerability in relation to the physical mitigation measures already employed. 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

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

B. Security Master Plan Implementation

While the Security Master Plan uses vulnerability and risk analysis as a foundation for developing guidelines, the Master Plan is not simply a report of current problems on campus. The objective of the 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 a 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.