Appendix L

City of Stockton, CA, Parking Operations Assessment

Parking Facility Security White Paper

April 2014

Kimley-Horn and Associates, Inc.

ENHANCING PARKING FACILITY SECURITY

AND ASSESSING SECURITY PROGRAM EFFECTIVENESS

By Dennis Burns, CAPP

This appendix on parking facility security is being presented in two parts. This first part reviews some of the basic security concepts specific to parking facility management and parking facility design. The second part will take a detailed look at assessing security programs in general.

Part One

Enhancing Parking Facility Security

Part One – Enhancing Parking Facility Security

Security within parking facilities is always a major concern. Statistically, over 90% of people attacked in parking decks are women who are alone. The longer they are alone the more at risk they are. The negative publicity associated with this type of crime can damage any business or institution. Liability is a key concern for garage owners and operators. There are many security techniques available for owners or operators of parking lots or garages. Most are common sense; others involve design issues that should be evaluated in the planning phases of new garage development.

Security techniques related to parking facilities are classified as either "***active"*** or "***passive***". Active security is defined as any technique requiring a human response, such as security patrols, guards, or audio-visual surveillance. Any device or technique not requiring a human response, such as lighting, fencing, glass-backed elevators and stairwells, etc. is defined as passive security. Passive security is more cost effective, and if done well, contributes to a patron's feeling of safety and comfort within a facility.

A facility designed with security in mind can incorporate many passive security features into the construction of the garage, and minimize *active security* costs. Among the features to be considered in the design/development phase of a new parking structure are:

- **Clear-Span Construction**

  Clear-span construction techniques reduce the number of columns within the structure creating better visibility and eliminating potential hiding places. In addition to these passive security advantages, the increased floor to ceiling height adds to improved facility wayfinding though enhanced signage placement options. Much depends on the structural system used.

- **External Ramping Systems**

  Some sites are well suited to a design that allows flat plates for parking with vertical ramping being external to the structure. This design increases visibility within the structure and has other way finding and pedestrian circulation advantages. In larger facilities, the same effect can be achieved even with internal ramps as illustrated in the photo below.

- **Glass-Backed Elevators And Stairwells**

  In general, the more open and visible confined spaces can be made the better. The general theory is that the criminal is less likely to attack standing in front of a window or open stair than in an enclosed area.

- **Security Screening/ Limiting Access Points Into The Facility**

  Restricting access to the parking facility on the lowest levels through the use of architectural screening or fencing better controls access into a structure and funnels pedestrians through designated points which can be more easily monitored. Also securing potential hiding places such as areas below stairs enhances facility security.

- **Lighting Design**

  Lighting is universally acknowledged as the most important security feature in a parking facility. Eliminating dark areas deters crime and promotes enhanced user comfort and improves the perception of safety. Good lighting permits the safe movement of pedestrians and vehicles within the parking facility, and it promotes internal facility way-finding.

  Light levels are generally not mandated by the building codes, other than certain minimum levels required for emergency egress. The industry standard for lighting design in parking facilities is established by the Illuminating Engineering Society of North America (IESNA). While not a legal building code, failure to comply with IESNA standards does carry significant liability.

  The IESNA standards are defined in terms of illuminance, or, in other words, the amount of light falling on an object. In general terms, parking structures require a minimum illuminance of 1 foot-candle and 10:1 maximum to minimum ratio for uniform light distribution. Stairways and lobbies require 2 foot-candles minimum. Vehicle entries and exits require 50 foot-candles during daylight hours to allow for safe transition from bright sunlight to the interior space.

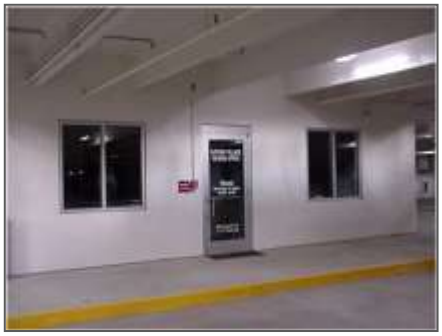
Typically, the white light provided by metal halide or florescent lamps is more comfortable to patrons because it is perceived to be brighter. Currently, florescent lighting is the least expensive lighting type to operate, due to lower energy demand and longer lamp life. Recent innovations have also made florescent fixtures more effective in cold weather climates.

Ideally, fixtures should be paired in each parking bay, spaced at approximately 30 feet on-center in each direction. This somewhat mitigates the shadows created by the parked cars, as well as reducing the lighting glare in the drive aisles. The paired fixtures improve the uniformity of the lighting and allow for a certain amount of forgiveness if a single lamp fails.

When used in conjunction with CCTV systems the color rendition of the lighting should be considered (for example, the whiter light produced by metal halide lighting may be preferable to the yellow tinted light produced by High Pressure Sodium fixtures if color cameras are used).

- **Security Office**

  Locating a security office within the parking facility is good way to add a significant security presence within the garage. This is especially effective if camera monitoring is visible by garage patrons.



- **Landscape Design**

  Landscaping should be kept low to the ground to minimize hiding places around the deck. Placement of trees, shrubbery and hedges can also restrict line of site vision for turning traffic if inappropriately placed or allowed to grow too tall, causing a safety hazard.

Other Security Enhancements

- Painting the interior of the facility is a good way to improve the "feel" of the deck. Painting or staining interior surfaces white makes better use of existing lighting by increasing reflectivity.

- The addition of convex mirrors in elevator cabs allows patrons to see, before entering, if anyone is hiding inside the cab.

- In general, eliminate hiding places within and around the garage. Small areas can be enclosed with chain link fencing to create storage areas and at the same time eliminate potential hiding places.

- Installing glass panels in stairwell doors improves visibility. (Check with local codes on whether stairwell doors are required to be fire rated. Typically they are not).

In Summary -

Developing a comprehensive program, with both passive and active security features, that is tailored specifically for each project is a key component to a successful parking operation.

Part Two

Assessing Security Program Effectiveness

Part Two – Assessing Security Program Effectiveness

INTRODUCTION

This article series on parking facility security is being presented in two parts. The first part reviewed some of the basic security concepts specific to parking facility management and parking facility design. This second part takes a detailed look at assessing security programs in general.

Building security has always been a concern for facilities management and parking professionals, but since the September 11th terrorist attacks and more recently the shootings on several university campuses we have been forced to constantly reevaluate campus and facility security issues. In this article, we'll provide you with a methodology to assess the effectiveness of the security programs at your facilities.

STAGE ONE - Conducting a Risk Analysis of Your Facility

A risk analysis consists of three major steps.

Step 1 - Conducting a Security Survey

The purpose of a security survey is to identify your organization's assets and their value and to identify threats to those assets.

Assets

The security survey should include walking through the facility and talking to the people who own it and work in it to determine the potential risks posed by the building's design and management. The physical areas to be inspected include the perimeter, offices themselves, and any areas where deliveries are received. Prior to a walk through, prepare worksheets or checklists to guide those conducting the security survey. It is also a good idea to take along copies of site plans, building plans etc. so that area of concern can be noted for easy reference.

Some of the assets that should be considered in the risk analysis include: employees, the facility itself, money, manufactured products, raw materials, intellectual property assets and industrial processes. As each asset is identified, the sources of external and internal threats to it should also be noted.

Threats

The most common external threats to a facility and the people in it include, but are not limited to, theft of equipment or data, assault, or perceived threats from loiterers.

One traditional means of evaluating external threats is to examine the community's most recent crime statistics to find out if the trends in rape, murder, theft, and

burglaries are heading up or down and how long the trends have been going that way, and why. Statistics of criminal incidents for each calendar year are summarized and published by category and jurisdiction by the U.S. Department of Justice in the Uniform Crime Reports. (All U.S. jurisdictions are required to report crime statistics to this department.)

Since September 11th, many facilities are also reassessing their exposure and their preparedness for bomb threats or threats to potential building contamination by chemical or biological agents. If there is one point that cannot be overemphasized, it is the value of being prepared. Do not allow a bomb incident to catch you by surprise. By developing a bomb incident plan and considering possible bomb incidents in your physical security plan, you can reduce the potential for personal injury and property damage. The website for the US Bureau of Alcohol, Tobacco and Firearms (ATF) is a good resource for developing a bomb incident plan for your facility.

Internal threats may come from disgruntled or dishonest employees. Examples of internal threats to assets are theft, fraud, destruction of property, arson, assaults, and crimes of passion resulting from interoffice romances. Companies should record all crimes, no matter how insignificant, that occur at the facility(ies) they own/operate.
Analysis of the incidents can reveal patterns of crime, which in turn can lead to identifying the perpetrators. Maintaining these records can also help owners avoid litigation for negligent security, as well as, support decisions to invest in new security measures.

Environment

Crime Prevention Through Environmental Design (CPTED) suggests that architects, facility planners, designers, and facilities/security professionals can create a climate of safety in a community or on a campus, by designing a physical environment that positively influences human behavior. These concepts can also be used to retrofit environments to address specific security issues as they develop or to address emerging concerns as conditions change.

CPTED builds on four key strategies: territoriality, natural surveillance, activity support, and access control.

- Territoriality:

People protect territory that they feel is their own and have a certain respect for the territory of others. Fences, pavement treatments, art, signs, good maintenance, and landscaping are some physical ways to express ownership. Identifying intruders is much easier in a well-defined space.

- Natural Surveillance:

Criminals don't want to be seen. Placing physical features, activities, and people in ways that maximize the ability to see what's going on discourages crime. Barriers, such as bushes, sheds, or shadows, make it difficult to observe activity. Landscaping and lighting can be planned to promote natural surveillance from inside a home or building

and from the outside by neighbors or people passing by. Maximizing the natural surveillance capability of such "gatekeepers" as parking lot attendants and front desk clerks is also important.

- Activity support:

Encouraging legitimate activity in public spaces helps discourage crime. A public break area or outdoor lunch patio creates activity and opportunities for casual surveillance. Any activity that gets people out and working together -- a company picnic, a tenant party, a civic meeting -- helps prevent crime.

- Access control:

Properly located entrances, exits, fencing, landscaping, and lighting can direct both foot and automobile traffic in ways that discourage crime.

These principles are blended in the planning or remodeling of public areas that range from parks and streets to office buildings and housing developments. Some institutions have incorporated these principles into more comprehensive facility and security approaches.

CPTED works best when integrated into a comprehensive crime prevention or security program. Several approaches can discourage undesirable vehicular traffic, including instituting perimeter and/or time-related restrictions, restricting access points, channeling traffic flow, monitoring in-coming traffic, etc.

A basic security planning Checklist is provided below:

BASIC SECURITY PLANNING CHECKLIST

- Assess overall physical security needs with regard to facility location, layout, design, construction, etc.
- Assess effectiveness of external/ internal controls with regard to an analysis of barriers, control points, entrances/exits, lighting, authorization levels, hardware, security devices, etc.
- Establish effective programs for personnel screening – particularly prior to employment. Establish programs for ongoing evaluation, monitoring, and assessment of personnel, especially those in high risk areas.
- Control and enforce authorization levels, key usage, access restrictions, sign-in/sign-out, opening/closing procedures, proper use of security systems, vigilance and surveillance, etc.
- Ensure full documentation of all security problems and violations.
- Develop levels of classification and restrictions (including written policies) on all sensitive material, etc.
- Establish procedures for handling/ safeguarding sensitive materials.
- Develop and enforce restrictions for employee access within the facility and around sensitive/high risk areas.

- Promote an ongoing program of monitoring and evaluation for the potential exploitation of persons with personal problems who work in sensitive and high risk areas.
- Establish effective ongoing security education training programs.
- Evaluate and plan for the possibility of electronic eavesdropping and ensure proper countermeasures.
- Use appropriate security systems, safes/vaults, and other anti-intrusion and theft devices.
- Develop a comprehensive business security planning program with ongoing evaluation and upgrade efforts.

A more comprehensive checklist is available upon request. Please send requests to dburns@carlwalker.com.

Step 2 - Estimating Probability

The second step in a risk analysis is to identify the probability that a risk will occur.

When assessing risks for security planning, employ this rule:

> "The more ways a particular event can occur, the greater the probability is that it will occur."

For example, to evaluate the risk posed to office equipment, ask and answer these questions:

- Is the equipment stored within secured rooms?
- Is the equipment secured within the room by anchor pads or other physical locking devices, or is it protected by electronic asset protection devices?
- How frequently do security patrols cover the area?
- How easy would it be for a thief to dispose of an item for profit?
- Is there a record of the serial numbers of the equipment?

Step 3 - Determining Criticality of Assets

When determining how critical an asset is to an organization, consider both the direct and indirect costs that will result from the loss of the asset. For example, many companies depend on the continuous and secure flow of electronic data inside and outside the facility. If the data flow were interrupted, the company would be unable to do business. The data, the facility where people use or manipulate it, and the connection lines the data travel over are all essential assets to the operation of many businesses. Therefore, data processing centers, telecommunication equipment, and the building infrastructure that supports them all have very high criticality.

Direct costs of the loss of an asset include permanent replacement, temporary substitution, or lost income. The indirect costs that should not be overlooked include

the adverse effect on the enterprise's reputation and employee morale, loss of goodwill, and possible employee turnover.

Establishing Security Needs

To complete the risk analysis, the information gathered from the security survey, probability estimates, and criticality decisions must be integrated to determine which assets are to be protected and which are not. Prioritizing assets and determining how vulnerable they are helps management decide the amount of resources to devote to security measures.

STAGE TWO - Selecting a Security System

We've just outlined how to conduct a risk analysis of your facility -- the first of three stages in developing an effective security program. Now, we'll continue with stage two: selecting a security system. A risk analysis should define which of your organizations assets require protection and which ones can remain at a level of risk your company is willing to tolerate. Once the risk analysis is complete and a need for an electronic security system has been established, the next step is to explore the types of systems available.

Because there are innumerable security systems with innumerable components, it's a good idea to break your research into four areas: access control, intrusion detection, surveillance, and command and control.

Access control

Access control systems regulate who is able to enter your building through devises such as electronic card readers and electronic locks on doors. Some of the most popular capabilities of access control systems include:

- User Card Number - a basic feature that identifies the access card user by a unique alphanumeric code defined by the system manufacturer.
- Anti-Pass Back - a time-delay feature that prevents a cardholder from passing his or her access card back through or under a closed or controlled door to be used by another person who may not be authorized to enter.
- Different or Multiple Access Levels - a feature that assigns different levels of access to different building areas and allows a facility to be partitioned to prevent access to some areas while simultaneously granting access to other areas. It can also define what days and hours occupants can use the access card.
- Historical Access and Departure Reports - a feature that provides reports of entries and departures from a building, or specific areas of a building, during certain dates and times.

Intrusion Detection

Intrusion detectors use sensors to detect either the open or closed status of protected points of entry, or the presence of a person in an area and the place where the alarm

terminates. Intrusion detection sensors are integrated into a system that transmits alarms to a processing location. The specific components, such as the status of latches, latch bolts or deadbolts (locked or unlocked); related power relays; switches; fittings; and keypads vary according to the type and level of protection.

Surveillance

Surveillance systems use video cameras and monitors to alert people to events that occur. Surveillance equipment is generally comprised of television cameras and monitors, video amplifiers, video switches, video tape recorders, audio tape recorders, and related cables, fittings and attachments. Closed-circuit television (CCTV) has long been associated with the security function. In the modern commercial building environment, its highest value is in providing an audit trail, which is critical in investigating a security breach or a violation of the law after such an event has occurred. (Very little crime is discovered through the CCTV surveillance system as it occurs.) Studies of individuals assigned to security consoles where CCTV cameras are monitored often indicate that console operators spend very little time watching the monitors; however, the gaming casino industry and retail environments use it to look for fraud or shoplifting. High security environments, such as the nuclear industry, military, and airports take a more vigilant approach to the use of CCTV in real-time environments. The features needed in a CCTV system depend on the purposes of security equipment as revealed by the risk analysis.

If the purpose of installing the camera is to reduce crime by immediately alerting an operator so the security force can be dispatched, the CCTV camera should be coupled with an alarm sensor device, such as a motion detector. If the purpose of the installation
is to record events, such as entries and departures, the recordings must be clear enough in terms of focus, resolution, and light levels to permit a positive identification of individuals and their activities.

If the video images and events will be used later in an investigation and criminal prosecution, the equipment must be able to produce the desired results. A management program must be devised to ensure proper archiving of the recorded events on videotape or CD-Rom for future use.

Command and Control

A central command and control station is required to manage the above-listed items and equipment. This station coordinates the control equipment and devices throughout a business's facility. This system includes a central console that coordinates the control equipment and devices required to manage the other equipment.

It also has central and remote signal processors that receive, transmit, discriminate, process, and convert signals from various security equipment into displayed and recorded intelligence or command and control functions. It has printing equipment to

make permanent records of significant changes of status and graphic display equipment to project two-dimensional views of protected areas.

STAGE THREE - Managing Your Security Program

The third and final stage in setting up an effective security program is managing the program.

Electronic security systems require more management after they are turned on than they do before and during installation, including attention to systems integration, the network they are connected to, the hardware, and the people using the system. Let's start with the people.

Occupant Orientation

All of your building's occupants should be made aware of how the system will operate during an emergency requiring building evacuation, local work rules, admittance procedures, and entry control system operation. In some cases, all personnel should view a brief videotape describing the local security and emergency procedures before they are issued access or identification cards.

Managing the System

The person responsible for managing a security system has duties to perform related to three primary areas: system administration, network operations, and hardware maintenance.

System Administration

Management of the access control systems and the intrusion detection and fire alarm systems are the key responsibilities of a security system's manager.

Managing the access control systems: Actual intrusions cause less than one percent of the alarms generated by electronic security systems. Many of these false alarms are triggered by faulty equipment, doors propped open, user error, someone exiting from an emergency door, an air conditioning or heating system activating a sensor, or a person trying to use a mechanical key to enter a door controlled by a card reader.

The system's manager should analyze and categorize the alarms and initiate corrective action to eliminate or minimize false alarms through prompt repair of faulty equipment, user retraining, adjustment of sensor sensitivity, or retrieval of mechanical keys from individuals who are violating access control procedures.

The access control system database usually contains two main types of information: the badge records of authorized individuals to locations where card readers are installed and the information used to automatically lock and unlock doors.

A security system manager should ensure that one person and a backup are assigned system administration duties, which include:

- Deleting system records of people who have left the payroll or tenancy, or whose entry privileges have expired. This task requires close collaboration with the human resources department and organizations responsible for hiring contracted workers.
- Printing hard-copy access reports from the system for a given period and retaining them for a specified period of time, usually three to six months.
- Periodically polling the system to determine whether cardholders have stopped using their cards or have left the payroll or tenancy without notifying the security department.
- Programming the system to deny entry privileges to a certain person or groups of people as business needs dictate.
- Programming door schedules to accommodate user requirements.
- Providing archived reports of entries and departures of specific individuals and matching the reports to video recordings of entries and departures for investigative purposes.
- Assuring that the time stamp for the entry control system is perfectly synchronized with the time stamp for the video surveillance system so that actual facility entry and departure times are properly matched with recorded times.

Managing Intrusion Detection and Fire Alarm Systems: Intrusion detection and fire alarm system databases will usually contain the name of each protected department within the facility (referred to as an account), its location, device numbers, contact names, telephone numbers, pass codes, and response directions. In addition, the database may also contain the name and phone numbers of the head person of the protected area. The database also requires updating when a new employee is hired, or a new device is added to or removed from the system.

Network Operations

The network established to link components of the access control and intrusion detection systems may consist of several different integrated transmission systems - copper wire, point-to-point fiber optic cabling, radio or microwave signals, and either proprietary or leased telephone lines that require maintenance.

Whether the transmission system is a single dedicated system or a fragmented system, arrangements must be made for maintenance and repair. Provision should be made for annual preventive maintenance, particularly when the transmission system is complex. During this annual inspection, all equipment, such as routers, switches, and transmitting or receiving devices, should be examined to assure that the equipment is operating according to specifications. Any equipment found deficient must be properly calibrated or replaced if necessary. Arrangements also must be made to provide immediate repair in case the network fails.

Hardware Maintenance

Most security system manufacturers and installers guarantee or warrant the reliable operation of their system and components for at least one year. Before a warranty period expires, be sure to execute a service contract with knowledgeable suppliers certified by the manufacturers to service the equipment.

IN SUMMARY -

Though our primary responsibilities may in the areas of parking and facility management, all of us need to sharpen our skills and knowledge of fundamental security issues. Success often lies in understanding the basic principles, developing collaborative relationships with security professionals and educating our customers on how to best protect themselves.

Acknowledgements:

The following articles were researched for the development of this article and the author gratefully acknowledges these experts.

Taking a Holistic Approach to Security
By David R. Duda, PE, CPP

Protecting Corporate Secrets
By Dr. Randy Gonzalez
Gonzalez is an instructor at the Sarasota Criminal Justice Academy in Sarasota, FL.

"Fear of Parking" & Pay Now ... Or Later
Dr. Randall Atlas, AIA, CPP, Vice President of Atlas Safety & Security Design, Inc.
Security Management (02/08) Vol. 52, No. 2

About the Author:

Dennis Burns is a Regional Vice President and Senior Practice Builder with Kimley-Horn and Associates Inc. Mr. Burns has over 28 years of parking operations, management and consulting experience.

Mr. Burns is the author of over 350 parking studies. His specific areas of expertise include: parking master planning, parking strategic planning, feasibility studies, supply/demand analysis, shared parking analysis, parking revenue control and operational audits, and parking system organizational development.

L. Dennis Burns
Regional Vice President and Senior Practice Builder
Kimley-Horn and Associates, Inc.
7740 N. 16th Street, Suite 300
Phoenix, AZ 85020
P: 602-944-5500 F: 602-944-7423 C: 480-290-5274
E: Dennis.Burns@kimley-horn.com

Appendix L:

DETAILED SECURITY PLANNING CHECKLIST

DETAILED SECURITY PLANNING CHECKLIST

1. **Access controls and facility surveillance aspects**
    - A. Identification and assessment of access controls, point of entry limitations, personnel vigilance, etc.
        - I. Types of controls and level of effectiveness in operations
            - a. In house security personnel: patrols and inspections
            - b. Alarm systems and anti-intrusion devices
            - c. Closed circuit television and electronic monitoring
            - d. Key control management and accountability
            - e. Levels of access and authorization
            - f. I.D. badges and recognition systems
            - g. Pre-employment screening and on-the-job monitoring
            - h. Security education and emphasis on enforcement
            - i. Other types of access controls
        - II. Perimeter and barrier protection
            - a. Natural barriers: landscape and terrain
            - b. Fencing: type and construction
            - c. Walls and ceiling construction: high risk areas
            - d. Gate facilities: security checkpoints
            - e. Frequency of patrols and security checks
            - f. Door and window locations and security devices used
            - g. Reception areas: location and control of entry
            - h. Employee surveillance and vigilance
            - i. Parking areas: entrance/exit, access to facility

2. **Identification of importance of product, process, information, etc.**
    - A. Importance of specific product, process, or service, and current security efforts applied to protect same
    - B. Levels of classification and authorization for access to specific product or service
    - C. Determination of how critical a security breach would be to company operations
    - D. Identification of critical office and work areas involving the use of the product, process, information, or service
        - I. How vulnerable are these areas at the present time?
        - II. How frequent is an evaluation made of critical areas?
        - III. How effective is pre-employment screening for persons in high risk or critical areas?
        - IV. What are the levels of authorization?
        - V. What levels of accountability are in force?
        - VI. Have security classifications been assigned?
        - VII. Has an assessment been made of the value, critical nature, and related impact on the company if a loss occurs?
        - VIII. What special advantages might be lost?
        - IX. Have effective countermeasures been implemented?

3. **External planning and assessment factors: security environments**
    A. Assessment of the business or facility in relation to the surrounding neighborhood, business district, industrial park, and other related setting
        I. Is good surveillance of the property possible?
        II. Are effective access controls in place?
        III. Is the structure located in a high crime area?
        IV. What has been the history of crime and/or security breaches?
        V. Is the facility isolated and located in a remote area?
        VI. If so, what has been done to protect/safeguard approaches to the facility? (Identification of visitors, vendors, etc.)
        VII. Are all possible access points monitored and protected?
        VIII. What would be the probable response time by police or in-house security staff if a security breach occurs?

    B. Assessment of factors pertaining to freedom of access and factors related to layout and design considerations
        I. Are external areas designed and developed in conjunction with security needs?
        II. Who is allowed access to the facility and during what times of the day? Levels of authorization?
        III. Have high risk areas, such as those containing trade secrets, confidential information, computer files, sensitive records, and documents been given special attention for security and protective needs?
        IV. What factors are specific to this particular operation?
        V. Are there any aspects of the facility in need of upgrade with regard to security?
        VI. How effective are the current security aspects of the following areas?
            a. Barrier controls, fencing, building design, etc.
            b. Lighting conditions for security illumination
            c. Obstructions to security patrols and surveillance visibility
            d. Exterior doors, access points, entrances, etc.
            e. Exterior windows and other openings
            f. Possible points of concealment and climbing aids
            g. Trash collection areas and disposal of documents, papers, etc.
            h. Alarm systems and related security devices
            i. Personnel, visitors, and others: control of movement, etc.

C. Assessment of the potential of unauthorized entry to high risk or sensitive areas
    I. Do neighboring facilities, structures, buildings, etc. present or create any observable security hazards? Could access control be compromised by an intruder gaining access from another building or facility?
    II. Could locking mechanisms be compromised?
    III. Do other openings create security problems?
    IV. Is there an effective program of lock maintenance and key control management?
    V. Has everyone been identified who has keys or other forms of access to high risk areas? Is the list up-to-date? Are there restrictions combined with levels of authorization?
    VI. If a locking system or other protective device is compromised, what procedures and/or actions are taken?
    VII. Are intrusion detection devices adequate? Could they be compromised? What changes would improve security?
    VIII. How effective is wall, ceiling, hallway, or office construction in preventing compromise of high risk areas?
    IX. Is there an effective level of employee vigilance?

4. Procedural security and policy formulation

A. Identification of essential needs for a written security policy with well-defined procedures
    I. Is there written company policy regarding security practices and procedures? Are there specific statements pertaining to the protection of company secrets, information, documents, etc.?
    II. Does policy incorporate specifics with regard to enforcement and penalties?
    III. Will the company prosecute?
    IV. Is policy translated into actual practice?
    V. Does the policy make an effort to cover all possible situations?
    VI. Do employees understand the policy? Is it made available?

B. Procedures and rules specify operational areas
    I. Are specific guidelines provided to all personnel with particular emphasis on operational areas?
    II. Do guidelines cover the locations and operations of the high risk and sensitive locations, such as: visitor control points; files and cabinets; labs and research; safes and vaults; library storage; copy centers; document storage areas; computer sites/centers; production/process areas; critical office areas; blueprint rooms; office equipment/machines; other special areas.

III. Are there checks and balances to ensure proper security regarding check-out, check-in, borrowing, loan, etc.?

C. Procedures, rules, and policies are clear-cut and understood with regard to all levels of operation in high risk locations within the company:
   - Employee orientation programs and training
   - Signed statements by employees attesting to policies, procedures, etc. (e.g. nondisclosure agreements)
   - Assignment of certain personnel (security staff) for monitoring, enforcement, etc.
   - Selective monitoring and evaluation (undercover officers, investigators, etc.)
   - Enforcement applied to everyone in a fair manner without regard to position or level in company
   - Security practices emphasized on regular basis
   - Opening and closing procedures
   - Log-in and log-out procedures followed closely
   - I.D. badges worn at all times where required
   - Centralization of access points, entrances, exits, etc.
   - Disposal areas and trash collection points monitored
   - Appropriate use of security systems and devices
   - Unannounced inspections and checks
   - Inventories and audits on regular basis

D. Procedure security planning

I. Is management satisfied that appropriate steps have been made to ensure reasonable security procedures to safeguard sensitive and critical information, processes, materials, etc.?
II. Is every effort made to ensure that personnel understand that a certain product, process, or information is classified as secret or confidential, or some other sensitive classification?
III. Has every effort been made to enforce and restrict the access to sensitive areas and materials? Have procedures been followed in a consistent manner?
IV. Have guidelines been published within the company listing those materials, processes, information, papers, etc., that are classified as sensitive and restricted? Are these provided for each specific group or project area?
V. Have levels of sensitive classification been established? (For example, "secret," "classified," "confidential," "restricted," etc.)
VI. Are restrictive signs posted in sensitive areas?
VII. How effective are current procedures with regard to:

a. Access controls
b. Opening and closing
c. Control of documents
d. Supervision/monitoring
e. Property control
f. Check-in and check-out
g. Control of contractors, vendors, repairmen, custodial services
h. Disposal/removal of records, papers, etc.
i. Key control and key usage
j. Locking and unlocking
k. Shipping/receiving controls
l. Storage of materials, etc.
m. Employee vigilance/surveillance
n. Security systems/devices
o. Other procedures and controls

5. Sensitive document security planning considerations

A. Assignment of levels of responsibility for the security and protection of sensitive documents and papers

I. Establishing internal controls, degree of security needed, and levels of responsibility

a. Who has primary responsibility to ensure the safeguarding of the sensitive documents and papers?
b. Do security personnel play a key role in such efforts?
c. What levels of clearance have been established?
d. How is responsibility delegated and how are persons held accountable for security requirements?
e. What is the current degree of security and what can be done to improve current conditions?
f. Is there a document control officer and what are his or her responsibilities?
g. Is there an on-going security education program?

I. Establishing internal controls and procedures

a. Has an identifications means been established to classify documents according to degree of sensitivity?
b. Are all documents covered by proper controls and audits, receipt verification, logging, etc. at all times?
c. Is a well-defined chain of custody maintained at all times?

d. Do control officer(s) ensure that documents are hand delivered to authorized persons with proper checks and balances?
e. Do all persons handling documents have proper clearances and were they properly screened through an effective pre-employment background investigation?
f. Do all storage facilities provide effective physical security?
g. Are all combinations, codes, or other access means to storage facilities protected at all times, and are these combinations changed periodically?
h. Are all files, safes, cabinets, etc. kept locked and secured at all times when authorized persons aren't present?
i. Are daily inspections conducted by control officer(s) to ensure that all materials are safeguarded and located in their proper locations?

B. Basic physical security planning

II. What measures have been taken to protect the areas containing sensitive documents and papers?

- Personnel controls
- Document controls
- Lighting security
- Door/window protection
- Identification controls
- External barriers
- Alarm systems
- Inspections/monitoring

6. Safes, vaults, and safe rooms

A. General considerations for safes and vaults

III. Review and analyze current usage, design, security aspects, related criteria concerning all safes and vaults

a. What types are used and how effective are they?
b. Where are they located and how well can they be protected?
c. Are they properly secured to a fixed position (if a small or portable safe)?

d. Are they being used appropriate to design and specifications as prescribed by manufacturer? UL ratings, etc.?
e. Who has the combination, how often is it changed, and how is the combination safeguarded?
f. How effective will the safes or vaults be against a burglary attack? What physical security needs are there?
g. Are any security alarm systems used to protect the safe or vault, including areas in which they are located?

. Procedures for safeguarding safe and vault areas
1. What access controls are used?
2. How frequently are these areas patrolled or inspected?
3. Are there levels of authorization required for access to the area or office location?
4. What other procedural safeguards are taken?

b. General considerations for a "safe" room (Note: A "safe" room could be used to safeguard small safe units, computer files, records, documents, and other sensitive material storage in lieu of a large vault if such would not be practical. Security alarms, maximum security hardware for doors, etc. would be critical to the design. The entire room would have to be protected on all sides, including roof and floor areas, with no other access points other than doors, in order to be effective.)
i. Has consideration been given to a special location within the facility for construction of a well protected, alarmed, and restricted "safe" room?
ii. If so, could small safes, sensitive files, documents, and related materials be placed within this room?
iii. Could a "safe" room be designed that would resist intrusion for several hours?

7. Personnel controls and security planning

a. Develop and identify critical needs with regard to screening, training, education, and access levels for all personnel
i. Screening and background investigations
1. Is someone assigned to conduct a thorough pre-employment screening for all personnel? Is this done at all levels where there is the possibility that contact will be made with sensitive/high risk information, materials, products, etc.?
2. Are all references thoroughly checked?

3. Are investigative tools such as a polygraph, special tests, or a combination of devices used in pre-employment screening?

ii. Supervision, monitoring, and evaluation
   1. Do supervisors provide an effective level of supervision at all levels? Do they set good examples for subordinates? Is there a good level of surveillance and vigilance in critical areas?
   2. Are periodic checks and inspections made by supervisors?
   3. Are personnel effectively evaluated in the handling of sensitive materials?
   4. Are all rules, policies, and procedures enforced?
   5. When a security violation occurs, is it documented?

b. Assess training, education, and other security needs
   i. Is there an effective security education program?
   ii. Are there any possible warning signs of potential problems with personnel in critical areas such as: personnel making threats, upset, dissatisfied, etc.; personnel with financial problems; personnel arriving earlier and/or staying later than normal; personnel with extravagant personal lifestyle or habits; personnel who avoid taking vacations, working weekends, etc.; other possible indications or problem areas.
   iii. What special security needs might be added to upgrade and enhance security of the area:
      - Additional barriers and access controls
      - Identification systems/I.D. badges
      - Restrictions on access and related control measures
      - Effective system of internal audits and inspections
      - Entry/exit screening packages, containers, etc.
      - Key control system/key control management
      - Strict enforcement of all security policies
      - Checks and balances/log-in and log-out controls
      - Change all locks and combinations when an employee leaves, transfers, terminates, etc. Change locks/combinations if a security breach occurs or is suspected
      - Upgrade security systems

The Security Checklist was created by Dr. Randy Gonzalez
Gonzalez is an instructor at the Sarasota Criminal Justice Academy in Sarasota, FL.