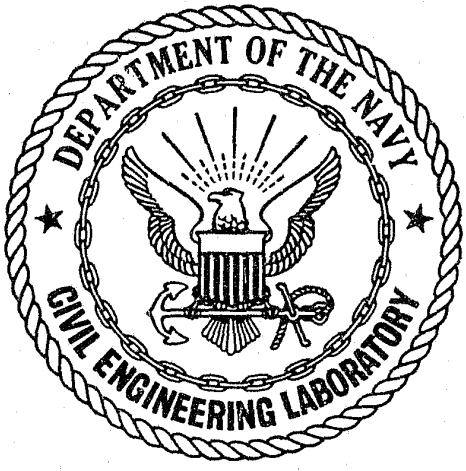


CR 78.002

CIVIL ENGINEERING LABORATORY
Naval Construction Battalion Center
Port Hueneme, California

Sponsored by
NAVAL FACILITIES ENGINEERING COMMAND

CONCEPTS FOR REDUCING CRIME, THEFT, AND DESTRUCTION OF NAVAL SHORE PROPERTY

September 1977

An Investigation Conducted by

WESTINGHOUSE ELECTRIC CORPORATION
NATIONAL ISSUES CENTER
Arlington, Virginia

N68305-77-C-0017

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER CR 78.002	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* CONCEPTS FOR REDUCING CRIME, THEFT, AND DESTRUCTION OF NAVAL SHORE PROPERTY		5. TYPE OF REPORT & PERIOD COVERED Final September 1977 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Robert K. Cunningham William D. Wallace Robert J. Haskell Lynne Helfer Palkovitz		8. CONTRACT OR GRANT NUMBER(s) N68305-77-C-0017
9. PERFORMING ORGANIZATION NAME AND ADDRESS Westinghouse Electric Corporation National Issues Center Arlington, VA		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS YF53.534.301.304
11. CONTROLLING OFFICE NAME AND ADDRESS Civil Engineering Laboratory Naval Construction Battalion Center Port Hueneme, CA 93043		12. REPORT DATE September 1977 13. NUMBER OF PAGES 163
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)* Naval Facilities Engineering Command 200 Stovall Street Alexandria, VA 22332		15. SECURITY CLASS. *(of this report)* Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Security, planning, crime reduction, facility, construction, crime prevention, environmental design

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

Concepts for crime reduction on Navy industrial type environments through control of environmental design are presented. Examples of crime prevention methods used in the public sector are discussed. Various opportunities for imput of physical security engineering and crime reduction factors into the planning, design and construction of new facilities are identified with reference to the Navy's Facility acquisition system.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

APPENDICES

CHAPTER 1. INTRODUCTION

1.1 General

This report is submitted in accordance with Contract No. N68305-77-C-0017 between the U. S. Navy Civil Engineering Laboratory, Port Hueneme, California, and the Westinghouse National Issues Center, Arlington, Virginia. It describes concepts currently being developed and applied in the public and private sectors for the reduction of crime -- emphasizing those that minimize theft of property by nonprofessional criminals -- and provides examples of conceptual applications.

Data presented represents a synthesis of information obtained from practitioners in the field of security, together with the experience gained by the Westinghouse National Issues Center during the first 3 years of its contract to develop Crime Prevention Through Environmental Design (CPTED) concepts sponsored by the Law Enforcement Assistance Administration (LEAA). The report provides an overview of the field of security engineering, rather than an indepth analysis of any one area. It is intended to provide an appreciation of security engineering principles and functions to architects, engineers, and Naval station operating personnel.

1.2 Scope

This report contains data on concepts and strategies being applied in the public and private sector that are potentially applicable to the planning, design, construction, and operational phases of Naval Shore Facilities. The objective to be achieved through application of these concepts and their related strategies is to minimize the theft of government property by nonprofessional criminals.

Security in the traditional military sense (i.e., as it relates to classified material and missions, and is typified by standards expressed in terms of locks and guards) is already extensively documented and is not a focus of this report, although the concepts described herein do apply to that area. There are also numerous publications and standards available that describe and specify security hardware and systems, including publications of the National Bureau of Standards; therefore, those areas are not detailed here.

Social strategies and interpersonal reactions are discussed to provide a better understanding of current activities in the environmental design field. Examples are provided to illustrate how security engineering principles can be applied, and how security engineering requirements can be incorporated into representative Navy documents and directives.

1.3 Security Engineering

As in any emerging field, there are divergent opinions regarding the areas of expertise to be considered as security engineering, as well as its primary focus of concern. As discussed in Section 1.4 and in Chapter 2, the concept of Crime Prevention Through Environmental Design (CPTED) is emergent in the public sector. This is, by definition, a wide-ranging field that includes both social and environmental concerns, and that concentrates on the interaction between the individual and his surroundings. *Security engineering*, as used in this report, is a subset of CPTED concentrating on the physical environment. It deals with spatial relationships and physical construction, emphasizing the denial of opportunity for criminal behavior and increasing the risks -- real or apparent -- of committing criminal acts.

Although physical security, as defined in OPNAVINST 5510.45B, United States Navy Physical Security Manual, is not specifically discussed in this report, it is considered a subset of security engineering. Concepts and strategies defined herein will increase physical security but are not a substitute for the specific mission-oriented protective measures outlined in OPNAVINST 5510.45B and similar directives.

1.4 Background

Throughout history, man has attempted to control crime through modification of his environment. For example, moats and fortress walls were built around medieval cities to reduce external threats; in the 17th Century, some 6,000 lanterns were installed on Paris streets as part of a crime reduction program; and in London, streets were cut through criminal-inhabited sectors and the criminal elements dispersed. Contemporary interest in environmental design as a crime prevention approach was stimulated by ideas presented in the 1960's and early 1970's by such researchers as Jane Jacobs, Elizabeth Wood, Shlomo Angel, and C. Ray Jeffery.

Jacobs' (1961) contribution was the theory that street surveillance is the key to crime prevention. She argued for diversifying land use to create more activity on the street, thereby creating more surveillance possibilities and stimulating informal social controls. In Jacobs' view, the essentials for crime prevention were a sense of community cohesion, feelings of territoriality, and responsibility for one's "turf."

Wood (1961), concentrating on public housing projects, suggested that paid surveillance, project police, and guards could never exert the control provided by an involved and interested community. She indicated that housing design must provide, at the very least, the

opportunity for communities to exercise social control. She supported designing for natural surveillance through visible identification of a family and its dwelling, and through enhanced visibility of public places.

Angel (1968) developed the critical intensity zone hypothesis: Public areas become unsafe not when there are either few or many potential victims present, but when there are just enough people on the scene to attract the attention of potential offenders, but not enough people for surveillance of the areas. He suggested alteration of physical configurations to concentrate pedestrian circulation and thereby eliminate critical intensity zones.

Jeffery (1971) noted the "failure" of prevention and the inadequacy of past prevention and rehabilitation models. As an alternative, he suggested that urban planning and design be employed to control crime.

These studies triggered widespread interest in the concept of crime prevention through environmental design. In 1969, the National Institute of Law Enforcement and Criminal Justice (NILECJ), the research center of the U. S. Law Enforcement Assistance Administration (LEAA), funded the first in a series of research projects aimed at assessing the relationship between the design features of particular environmental settings, citizen fear, and vulnerability to crime. The work of Oscar Newman (1972) suggested that the physical design features of public housing affect both the rates of resident victimization and the public's perception of security. These design features included building heights, number of apartments sharing a common hallway, lobby visibility, entrance design, and site layout. The research also indicated that physical design can encourage citizens to assume behavior necessary for the protection of their rights and property. These concepts led, in Newman's terminology, to the establishment of "defensible space."

Thomas A. Reppetto (1974) studied residential crime patterns and examined possibilities for controlling the crime problems. He concluded that future research should be directed towards the development of a crime prevention model that would blend together the deterrent effects of the criminal justice system and citizens' anticrime efforts and that, perhaps, improved environmental design would be the most effective way.

In 1974, NILECJ initiated the Crime Prevention Through Environmental Design (CPTED) Program. The overall purpose of the effort was to demonstrate and evaluate the environmental design concepts in those environments (schools, residential, and commercial) that had not been addressed in previous studies.

As part of this ongoing program, CPTED-related concepts were critically reviewed and their interrelationships were defined. Based upon these concepts, strategies were developed for their practical application. The scope of the CPTED Program includes social interaction and concentrates on fear-producing crimes (Part I Crime Index offenses*); many of the concepts, and their application, are relevant to the scope of this study.

Paralleling this development of crime prevention through environmental design concepts in the public sector was a realization in the private sector that there existed a need to formally *include security* in all planning and operational activities. The growing focus, and specificity associated with this realization, was reflected in the applicatory literature being published.

In 1971, M. Liechenstein, in his Designing for Security, pointed out that much interdisciplinary research was required to determine what physical and psychological ingredients would combine to create good security. Observing that while there existed little in the way of formalized procedures designed to create good security, he noted that there was a great deal of knowledge as to what constituted poor security. In support of his concern, he further characterized the state of security planning as being chaotic. He noted that general neglect of security was supported by untimely and weak interaction between those agencies that could both influence and profit from improved security and that the essential role of the architect in security planning has not been recognized. Architects did not design for security, nor did building permit officials insist on it. He believed that police and *security experts should be involved during facilities planning sessions so that security requirements could be considered in construction design.*

By 1974, H. S. Ursic and L. E. Pagano, in their Security Management Systems, identified organizational security as a specialized field, somewhere between an art and a science, although they acknowledged that no attempt had yet been made to apply a scientific approach to security problems. They recommended that security progress in a scientific environment, and that industry deemphasize traditional

---

*As defined and reported in the Federal Bureau of Investigation's Uniform Crime Reports, published annually. The Part I offenses include murder, nonnegligent manslaughter, rape, aggravated assault, robbery, burglary, larceny, and auto theft.

experiences as a preparation for meeting security requirements and organize vigorous educational programs for the future. In 1975, T. J. Walsh and R. J. Healey, in their Protection of Assets Manual, took the next logical step and stated that *in the construction of new facilities, as well as in the rebuilding of existing facilities, physical security controls should be included as an essential element in the architectural design.*

At the same time, some of the more progressive commercial/industrial enterprises were recognizing the need for security planning and were quietly developing their own pragmatic strategies in an effort to reduce their losses due to theft, or to devise less costly means of protecting their assets. Since successful approaches were considered a competitive advantage, these concepts were not widely publicized. Nevertheless, these industrial practices represent real-world applications for designing the physical environment to control what most corporations acknowledge to be their major crime problem -- theft. Although these strategies may deter the professional criminal, they are aimed more specifically at preventing crimes of opportunity, and industry has found that control of such losses can have a decided impact on product costs and corporate profits.

1.5 Summary

The objectives of this report are to make the Naval establishment aware of the current concepts and strategies in the field of security engineering and to recommend how security engineering can be included in the Navy Facilities Planning Cycle. In support of this objective, applicable Crime Prevention Through Environmental Design (CPTED) concepts are described in Chapter 2, and commercial security engineering practices are described in Chapter 3. Chapter 4 discusses the Navy Facilities Planning Cycle and recommends means by which security consciousness and practices can be incorporated. Chapter 5 discusses some of the actions recommended as part of any Navy security engineering program, and Chapter 6 summarizes the report's findings, conclusions, and recommendations. Appendices A through D present security engineering concepts and strategies applicable to specific types of construction or renovations projects. Appendices E and G provide a list of consultants active in the field and an annotated bibliography of CPTED and security engineering, respectively. A more complete discussion of the CPTED Program, including social concepts and illustrations of CPTED strategies, is provided in Appendix F.

CHAPTER 2. CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

2.1 Introduction

The focus of security traditionally has been on the intruder and on the prevention of crimes of violence. This focus is reflected in current practices, literature, and most research efforts. This emphasis could be justified in the past since it complemented the barriers to crime imposed by the existence of the stable family or community group. With the mobility of the 20th century, however, the peer group pressures which mitigated against crime have largely disappeared, and crime -- including assaults, theft, and so-called "white-collar" crime -- is now traceable to members of the group itself. This trend has been tacitly recognized in the research area, and control concepts that are aimed at control of groups of people rather than the individual professional criminal are being developed. The most exhaustive of the current research studies in this area is being conducted by the Westinghouse National Issues Center. It is supported by the Law Enforcement Assistance Administration (LEAA) and is entitled Crime Prevention Through Environmental Design (CPTED). As previously noted, CPTED concentrates on Index crimes, and its strategies apply to the physical, social, environmental, and law enforcement areas. The CPTED design concepts described in this chapter are applicable to security engineering and should be considered in any security engineering application. A more complete description of the CPTED Program is provided in Appendix F.

2.2 CPTED Design Concepts

Four design concepts and associated strategies are described under the CPTED Program; two of these -- access control and surveillance -- are directly applicable to the security engineering area. The other two, activity support and motivation reinforcement, fall, by definition, into the operational area, but are applicable in the sense that physical design and spatial relationships should support their implementation. They should, therefore, be considered during facility design as would any proposed use of the facility being constructed. All four concepts unavoidably overlap; in fact, a single design strategy may reflect different design concepts depending upon its environmental setting.

The four design concepts and illustrative strategies are discussed below. Although they have been developed for the public sector, they are applicable in any security setting. Strategies based on these concepts and directly applicable to the Navy establishment are found in Appendices A through D.

2.2.1 Access Control

Access control is primarily directed at decreasing exposure to criminal activities. In essence, it operates to keep persons out of a particular locale if they do not have legitimate reasons for being there. In its most elementary form, some access control can be achieved in individual dwelling units or commercial establishments by use of adequate locks, doors, and the like (i.e., the group of design strategies known as target hardening).

However, when one moves beyond private property to public or semipublic spaces, the application of access control becomes more complicated. Lobbies of apartments, office buildings, or schools are often open to the public and, consequently, to those persons who will commit offenses if the opportunity arises. One strategy is to station guards at entrance points to screen visitors, but this is both costly and potentially counterproductive if arbitrary decisions must be made.

Access control is most difficult to achieve on streets and similar areas that are entirely open to public use. In some areas, such as neighborhoods of tightly knit ethnic groups, the streets are effectively denied even to certain noncriminal outsiders by the imposition of social barriers. However, there are other, more legitimate techniques for limiting access in areas nominally open to the public. Physical barriers imposed by natural forms (e.g., rivers and lakes), existing manmade forms (e.g., railroad tracks, parks, vegetation, highways, and cemeteries), and artificial forms designed expressly as impediments (e.g., street closings and fences) serve to restrict or channel movement and to limit access.

Many burglars and robbers display environmental preferences, both physical and social, that can be frustrated by the creation of psychological barriers. These barriers may appear in the form of signs, parkways, hedges -- in short, anything that announces the integrity and uniqueness of an area. The hypothesis operative in creating psychological barriers is that targets that seem alien, mysterious, or difficult may also seem unattractive to the potential offender. As a paradox, the hypothesis can work when areas -- by their clear legibility, transparency, and directness -- discourage the potential offender because of users' familiarity with each other and their surroundings, and the visible absence of places to hide or conduct furtive acts -- in short, because of the conspicuous cohesiveness of the area.

In facility design, the access control concept involves restricting the movement of personnel to the minimum necessary for legitimate purposes. On a base, support facilities would be located near an entrance and dependent housing. Shipping and receiving points would be consolidated and routes to and from these areas would be as direct and short as possible. Outpatient facilities in a hospital would be near an entrance. All of these are examples of access control.

Because any strategy that fosters access control is also likely to impact upon egress, careful consideration should be given to access control strategies. They may not only limit the egress of offenders, but also hinder the mobility of potential victims.

2.2.2 Surveillance

Although similar to access control in some respects, the primary aim of surveillance is not to keep intruders out (although it may have that effect) but, rather, to keep them under observation. Surveillance increases the perceived risk to offenders, and the actual risk if the observers are willing to act when potentially threatening situations develop. A distinction can be made between organized surveillance and natural or spontaneous surveillance.

2.2.2.1 Organized Surveillance

Organized surveillance is that which is provided by a dedicated source, such as a police patrol, in an attempt to project a sense of omnipresence (i.e., to convey to potential offenders the impression that police surveillance is highly likely at any given location). The effectiveness of this particular technique may vary greatly with geographic considerations, temporal and crime-specific factors, and the efficiency of the police themselves. There is some evidence that community/police cooperation may be increasing spontaneously, and the spread of such indicators might prove a potentially important trend.

Organized surveillance also can be achieved by nonhuman techniques such as closed-circuit television (CCTV) or alarms. Noteworthy success is reported to have been achieved in certain residential complexes where the CCTV surveillance channel can be dialed on residents' individual sets; this medium provides an additional window on the world and even serves to promote social interaction. Better results might be achieved if the surveillance function of the CCTV channel or channels were transformed or subordinated into one of several communications functions of the same system, so that crime surveillance could occur as a natural byproduct of a system actually serving several positive purposes.

Security engineering ensures that traffic routes and design of facilities support the use of patrols, and that provision is made for electronic surveillance support during facility design or renovation. Basically, security engineering supports the use of organized surveillance.

2.2.2.2 Natural Surveillance

Natural surveillance is that provided by nonsecurity resources and can be achieved by a number of design techniques, such as channeling the flow of activity to put more observers near a potential crime area, or creating a greater observation capacity by installing windows, enclosing a staircase in glass, or using single-loaded corridors. Proper attention to the design concept can lead to a reduced number of conventional guard posts and greatly enhanced security. Relocating a bicycle rack so that it can be observed through a window by the bicycle owners in the normal course of their work is an application of this concept.

2.2.3 Activity Support

The general design concept of activity support involves methods of reinforcing existing or new activities as a means of making effective use of the built environment. This design concept originates in the observation that in a given community, social and physical networks and nodes exist as latent, often underused, resources capable of sustaining constructive community activities. Support of these activities can bring a vital and coalescing improvement to the community, along with a reduction of the vulnerable social and physical gaps that permit criminal intrusions. Such an approach might focus on a geographic area (e.g., block, neighborhood, city sector), a target population (e.g., vulnerable elderly victims, opportunistic youthful offenders), or an urban system (e.g., health delivery, transportation, zoning).

Security engineering implements this concept by locating playgrounds where the children's parents can observe them at play, by placing reading or activity rooms near a building entrance, or by designing attractive mini-malls to foster constructive social activities.

2.2.4 Motivation Reinforcement

In contrast to the more mechanical concepts of access control and surveillance that concentrate on making offenders' operations more difficult, motivation reinforcement seeks not only to affect offender behavior relative to the built environment but to affect offender motivation by increasing the risk of apprehension and by increasing the

potential offenders' involvement in and identification with the physical and social environment that may be the object of criminal activity. Furthermore, this concept also emphasizes positive reinforcement of the motivation of the nonoffender community by increasing territorial concern, social cohesion, and general sense of security.

These strategies promote the transformation of human energy from illegal or destructive activity to legal or constructive outlets.

For example, the Philadelphia Parkway School Program extends high school students' educational activity during and after school hours by providing work and study in the public and private facilities located in downtown Philadelphia. These activities include work/training programs in apprenticeship roles; special projects in the public museums, libraries, and recreation facilities; and a wide range of other constructive activities.

The Parkway School Program is an ingenious way of making better use of existing, but not optimally used, resources on a large-scale multiuse basis. In a crime prevention sense, it is self-evident that potentially mischievous high school students engaged in learning a trade or performing a project will be diverted from participating in street crime. Similar programs in other modes could potentially involve other unproductive or excluded groups of the population.

Implementing the concept of motivation reinforcement falls primarily within operational channels. As with activity support, this concept influences facility design when activities that may be implemented can be supported by facility design.

2.3 Summary

Four design concepts have been defined under the CPTED Program. Two of these, access control and surveillance, are directly applicable to security engineering. A third, activity support, is applicable in that it should be considered during facility design. The fourth, motivation reinforcement, falls within operational prerogatives, and will normally have little influence on facilities design.

CHAPTER 3. COMMERCIAL PRACTICES

3.1 Introduction

This chapter describes security engineering practices that are being followed in the commercial sector. While such commercial practices are not so well documented as are the concepts being developed in the CPTED area, it should be noted that the reasons for their adoption directly correlate with the objectives established for this study -- the reduction of losses due to theft by nonprofessional criminals. Losses to industry due to theft amount to millions, perhaps billions, per year. It has been estimated that 80 percent of these losses are due to theft by employees or others who are authorized access to the area from which the theft occurs. While dollar value of each theft is low, and they are not the type that are headlined in the news, they significantly affect profitability. In fact, an estimated 30 percent of all business failures, nationally, are attributed to employee dishonesty.

Responsibility for security planning and operation for larger companies in the private sector is usually decentralized to the operating entities (e.g., factories, complexes) with support from a corporate-level security office. This security office performs a normal staff function in that it helps establish corporate policy, conducts training courses, and participates in corporate planning. In addition, the services of the office are available throughout the company to assist in the resolution of security or security-related problems. As a result, its personnel necessarily become involved in many divergent areas and acquire a practical knowledge of corporate operations, problems, and solutions. It is in this office that the impetus for security engineering is found.

At the plant level, responsibility for security is often fragmented. Conventional security (e.g., guards, gates, locks) and investigations are the responsibility of a security officer (or an operations manager, administrative officer, personnel director, or other) and his staff. Others involved in the broader area of theft prevention and loss reduction are the line and staff managers, accountants, foremen, and personnel managers. Successful security and loss prevention require that all such persons have security-related knowledge since the best results are obtained when all participate in the process of designing as well as operating their facilities.

It is also important to note that, for a technique or concept to receive acceptance in the commercial area, it must in some way enhance operations; even in this decade of growing social awareness, this means

decreased cost or increased effectiveness. Therefore, it is significant that practices and policies that implement security engineering strategies are receiving growing acceptance by the more progressive corporations.

While not directly applicable to security engineering because they fall in the operational area, there are many commercial practices that are being implemented as security consciousness increases. For example, preemployment screening to eliminate potential offenders has proven extremely effective. This technique, although not directly applicable to Navy personnel, does have applicability in the industrial complex area. Other practices receiving more emphasis in the commercial area, such as assignment of responsibility for tools and sign-out procedures, have been longstanding military practices. While not within the scope of this report, the increased attention to security evident in the operational area due to security engineering training may be one of the major benefits obtained.

3.2 Training

It is accepted in the commercial sector that all individuals who have responsibility for any component of the security system should be trained in their particular function. The proper integration of the abilities of all members of the organization with the physical resources and available technology determine the success and quality of a security system. The numbers and types of individuals to be trained or to be consulted in the planning cycle increase as the effort progresses.

The training of the operators is usually done by the corporation. Short, formal sessions are augmented by on-the-job training and security seminars. Instructors are corporate security personnel and outside consultants. Training of the security personnel is a combination of on-the-job training and formal instruction at one of the many colleges, private corporations, and professional associations that have (recently instituted) courses and/or seminars to provide the security manager with the tools to implement his program effectively.

It is important that proper security training be provided to more individuals than merely the security manager. *A proper security program begins at the initial site selection. Therefore, planners, architects, and others involved in the process must be made aware of security design applications and ensure their consideration and use from the outset; deficiency inspectors must consider security when determining the usefulness of an existing facility.* Employment personnel must be aware of security implications when screening recruits.

3.3 Commercial Concepts

The primary goal of commercial security engineering is to decrease loss and increase effectiveness. *Experience has convinced corporate management that this can best be accomplished by involving security representatives in every phase of the facility development cycle. Modifications that can be made at no increase in cost during initial planning may become prohibitively expensive or impossible at a later date.* What these modifications are will vary depending upon the specific project being reviewed; however, an analysis of the strategies being applied leads to the identification of the following principles or concepts:

- To be effective, security must be implemented before construction starts and maintained thereafter (e.g., key control can be lost if keys are not controlled during construction).

- The use of a removable core locking system or of "construction" cores should be considered as a means of restoring key control on completion of construction.

- Site perimeter security must be designed for the circumstances present (e.g., adjacent schools, trailer courts, commercial, and residential areas all represent divergent problems).

- Parking lot location is a crucial element of pilferage control. They should be convenient, but routes to and from the lots must be under surveillance. Foot traffic to and from the lots should be restricted to a few designated entry points by the judicious use of fences or other barriers.

- Commercial and visitor parking and traffic flows should be separate from employee parking.

- The number of professionally manned guard posts can in some cases be reduced by placing secretaries, receptionists, etc., so that they maintain surveillance over entry and exit points.

- Unsupervised entry and exit points (doors) should be locked, eliminated if not required, or designed as emergency exits with alarms installed to signal their use.

- Shipping and receiving points and associated traffic should be separated if possible.

- Fencing is sometimes counterproductive. It is less costly to use open landscaped areas as long as the landscaping is planned so as not to provide hiding places or concealed routes of entry.

- Security design, hardware, and operational policies are cheaper and often more effective than guard posts and fences (one 24-hour guard post requires 4 1/2 men at a cost of $50,000 to $100,000 per year). Design and hardware expenditures are a one-time cost.

- Early coordination with local law enforcement officials is required to obtain cooperation and help in designing site security.

- Vehicle movement should be limited by the use of artificial (but natural) barriers (e.g., trees, bushes, mounds).

- Areas around buildings should be clear for about 100 feet to enhance surveillance.

- Wiring and spare conduits should be sufficient to support the maximum need for security hardware foreseen for the life of the building.

- Where attempts at forcible entry through exterior walls are likely, building construction should be of tilt slab or other attack resistant construction, not cinder block.

- When designing the facility, high-value, sensitive, and pilferable item locations should be identified and so located as to inhibit loss (e.g., food, beverages, clothes, drugs, firearms).

- Facility management and security personnel must participate in security engineering, be trained in security principles, and assist by developing and implementing complementary operational procedures.

- Security engineering should consider and design three successive barriers to penetration:
  - The perimeter and structure relationship.
  - The building perimeter (lights, surveillance, construction).
  - Internal security and sensitive item location.
- A thief needs knowledge, time to plan, the necessary equipment, and an opportunity to work undetected. Denial of any of these will reduce or stop losses. Security engineering requires consideration of how best to deny each.
- Quality hardware and construction pay. It makes no sense to install an elaborate security system around a particle board door with a cheap lock or to install a good door and lock in a sheet-rock or other type of easily penetrated wall.

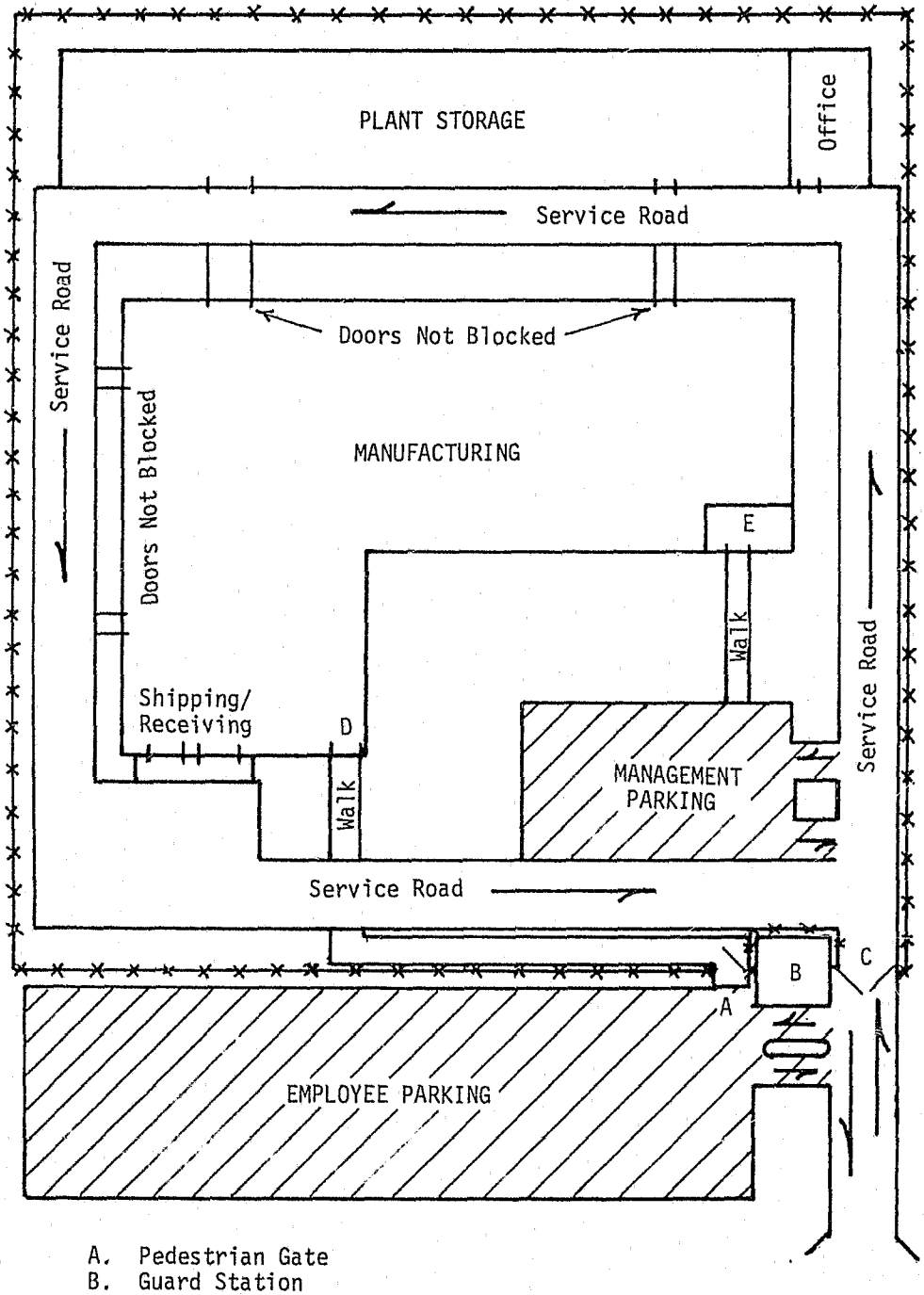
3.4 Design Features

3.4.1 General

A better appreciation of the effect that application of security engineering concepts will have on facility design is provided by examination of real-world examples of good and bad design. Because of the proprietary manner with which such costs are treated in industry, actual data on relative costs/benefits could be obtained for only one set of designs -- that shown for two comparable site plans. However, even for that example, conclusions regarding what factors contribute to the differences cited have not been drawn officially, and permission to credit the source has not been given. The other designs shown are presented as examples and no cost/benefit data are available.

3.4.2 Industrial Site Planning

Figure 3-1 shows the site plan for plant A, which is currently operating in the northeastern United States. It is typical of many industrial facilities designed using the "island" or "enclave" process and has what many consider to be good security design. It was built in the late 1950's, and can be said to represent the philosophy that security is a quasi-law enforcement activity that requires physical



A. Pedestrian Gate
B. Guard Station
C. Vehicular Gate
D. Employee Entrance
E. Receptionist

Figure 3-1. Plant A, Traditional Design

security systems and emphasizes apprehension. In this instance, apparatus and procedures were installed to deny unauthorized access, as well as to detect and apprehend persons who succeeded in gaining unauthorized access. At this site, the rate of property loss by theft is reliably estimated to be $2,500 per year, exclusive of hand tools of nominal value.

Plant B, which is also in the northeastern United States and under the same corporate management, produces similar products, and utilizes what might be classified as CPTED security engineering design features. Here, losses were reliably estimated to be $100 per year. At plant B, there is no perimeter fence, a nominal security guard presence at shift change and nonworking hours only, and minimally prudent physical security of property commonly subject to theft.

Security operating costs at plant A are $3,800 per month, exclusive of depreciation of capital costs of such major items as security fence and closed-circuit television. Security costs at plant B -- where losses are 1/25 of those at plant A -- are $1,950 per month, or about one-half of those at plant A. Total direct, annual security costs at plant A are therefore $48,100 (direct costs plus loss), not counting capital investment costs; at plant B, total costs are $23,500.

It is significant to note that neither plant experienced losses directly attributable to outside sources. Neither plant produces, stores, nor has access to material having a government security classification. The respective site plans for plant A and B are shown in Figures 3-1 and 3-2.

3.4.3 Access Control Application

There are numerous methods of access control. Office buildings with underground parking can be illustrative of both good and bad access control design concepts. Figure 3-3 shows the lobby arrangement of a building in which designated elevators are programmed to operate only between the lobby and parking levels; others operate between the lobby and the upper working levels. Therefore, persons entering the building from the parking level must exit the elevator at the lobby floor and, if proceeding to a higher level, board another elevator. The receptionist or security guard station is located so that the doors of all elevators, the building entrance, and lobby floor corridors are all in view. Persons entering the building from any access must pass this station; visitors, and employees during nonbusiness hours, must sign in and out. On request, escort is provided to persons proceeding to underground parking.

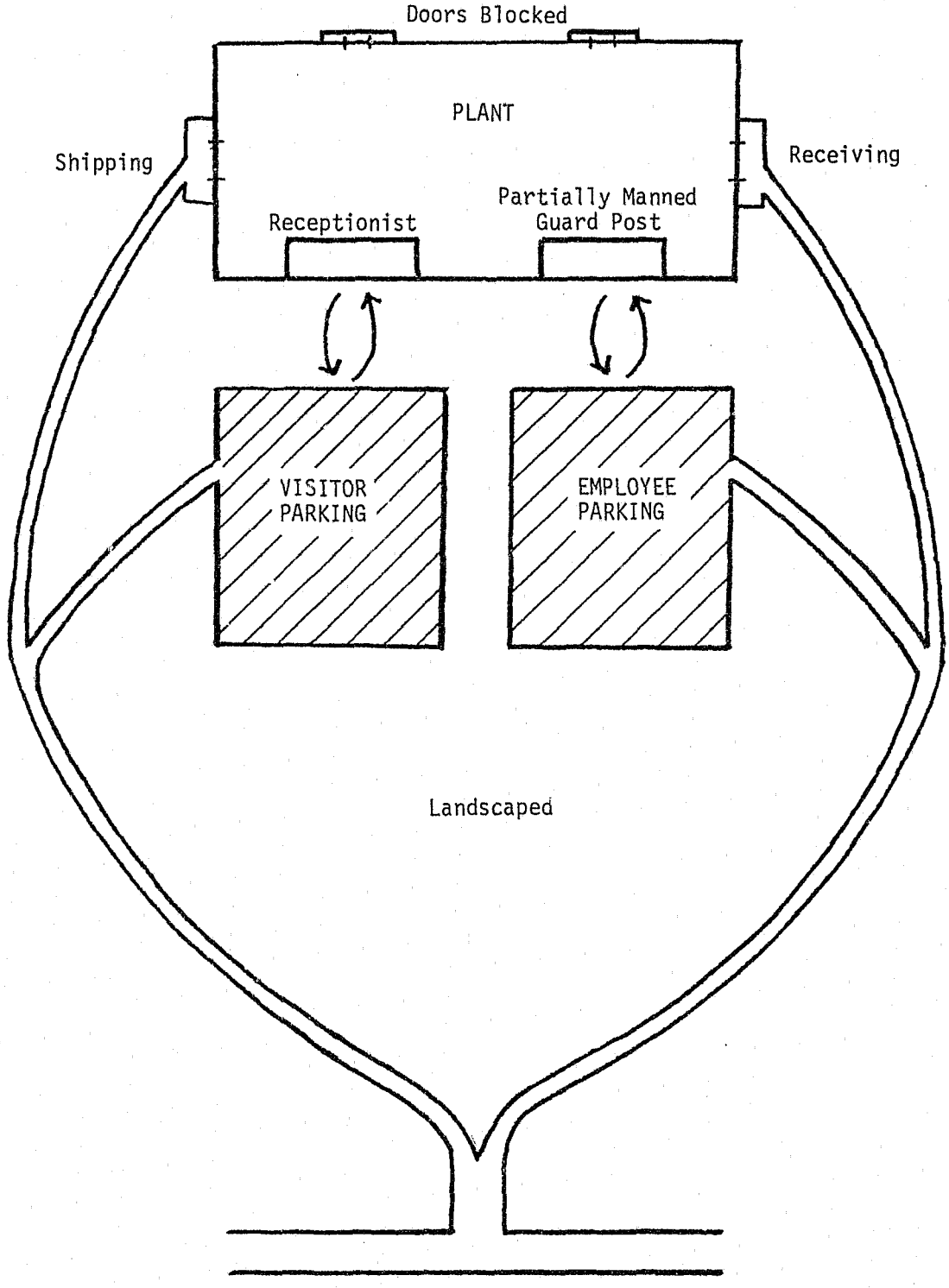
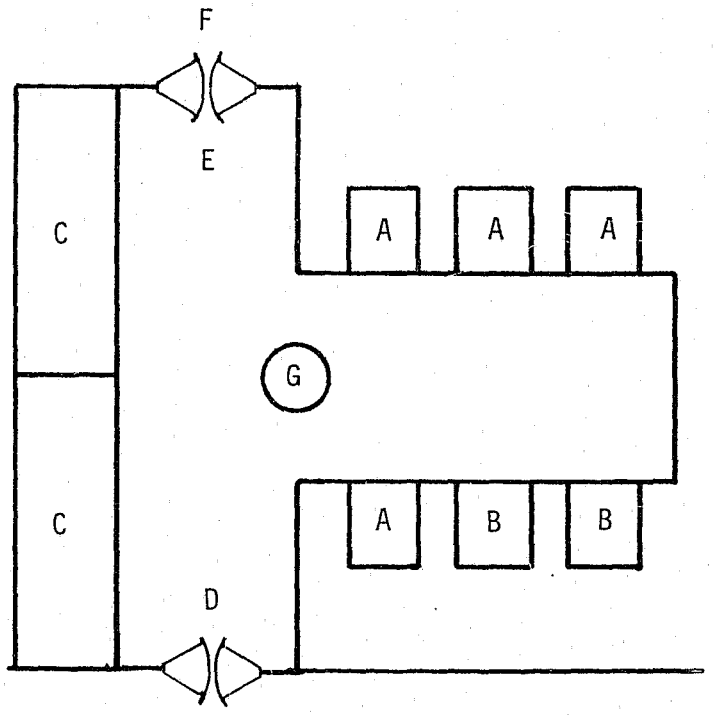


Figure 3-2. Plant B, Modern Design



A. Elevators serving lobby and specified floors above

B. Elevators serving lobby and floors below

C. Rest Rooms

D. Building Main Entrance

E. Main Floor Corridor

F. Controlled access/egress door

G. Receptionist/Security Guard station

Figure 3-3. Effective Office Building Access Control

In a commercially operated building that houses offices of the same corporation, access control is frustrated by building design and mode of operation. The arrangement of the lobby is shown in Figure 3-4. While all elevators are programmed to make a short stop at the lobby floor en route up from the parking levels, they then proceed to the office floors above. The elevator banks at the lobby level can be accessed from any of three entries. The security station provides no visibility to the elevators and to only two of the three entrances. Moreover, the security station is not manned around the clock. Therefore, access to the lobby and upper floors can be gained from the parking levels and at least one lobby-level entrance at all times without benefit of surveillance; at times, all access is free of observation. Although offhours sign-in and sign-out is specified and accommodated, it is not enforced. It is easier to leave unobserved than it is to enter because the elevators are not programmed to stop at the lobby on downward runs to the parking levels.

3.4.4 Surveillance

Office building surveillance is improved by situating support personnel so that they can observe halls and entrances. In some instances, a window wall or glass door is sufficient. In factory or warehouse facilities, similar techniques are enhanced by strategic location of the desks or offices of supervisors and foremen. In some instances, the elevation of these supervisory stations improves surveillance as well as communication and control functions.

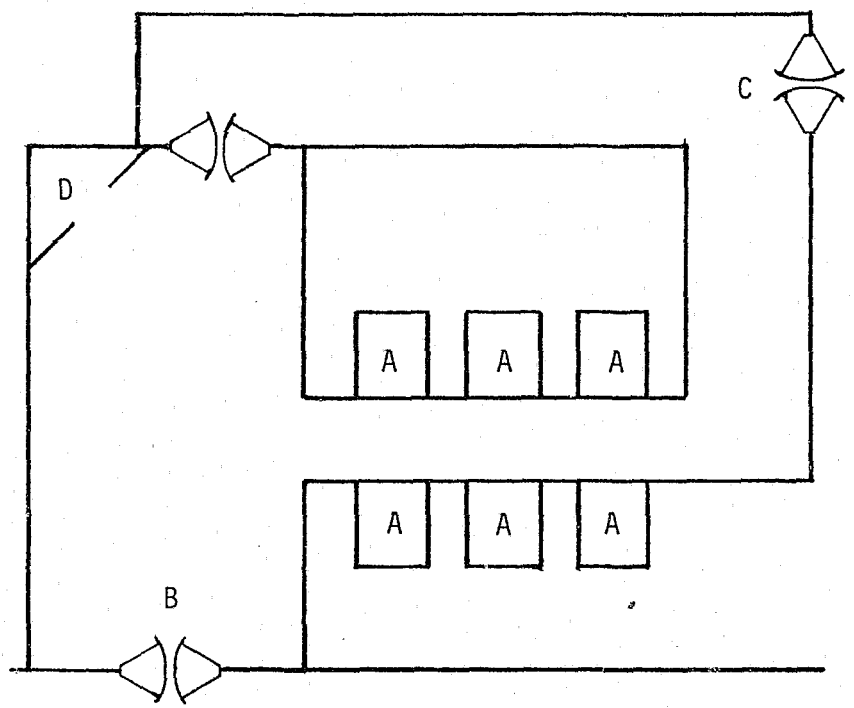
The shift of traffic flow and relocation of off-duty activity areas have been used successfully to improve surveillance of vulnerable areas in manufacturing and warehouse facilities.

3.4.5 Shipping and Receiving

The shipping and receiving functions constitute a point of contact by persons external to the operations, offer tempting targets at a vulnerable point in the line of control, and provide opportunities for collusion between persons internal and external to the operation.

To minimize vulnerability, a two-way point of control should be placed between both shipping and receiving and other elements of the operation. Shipping and receiving should be physically isolated from each other, and external traffic should be routed to minimize access.

An example of poor shipping and receiving design is illustrated in Figure 3-5, the layout of a large industrial complex in the mid-Atlantic region.



A. Through elevators from below ground to working floors

B. Main Entrance

C. Side Entrance

D. Guard booth

Figure 3-4. Ineffective Office Building Access Control

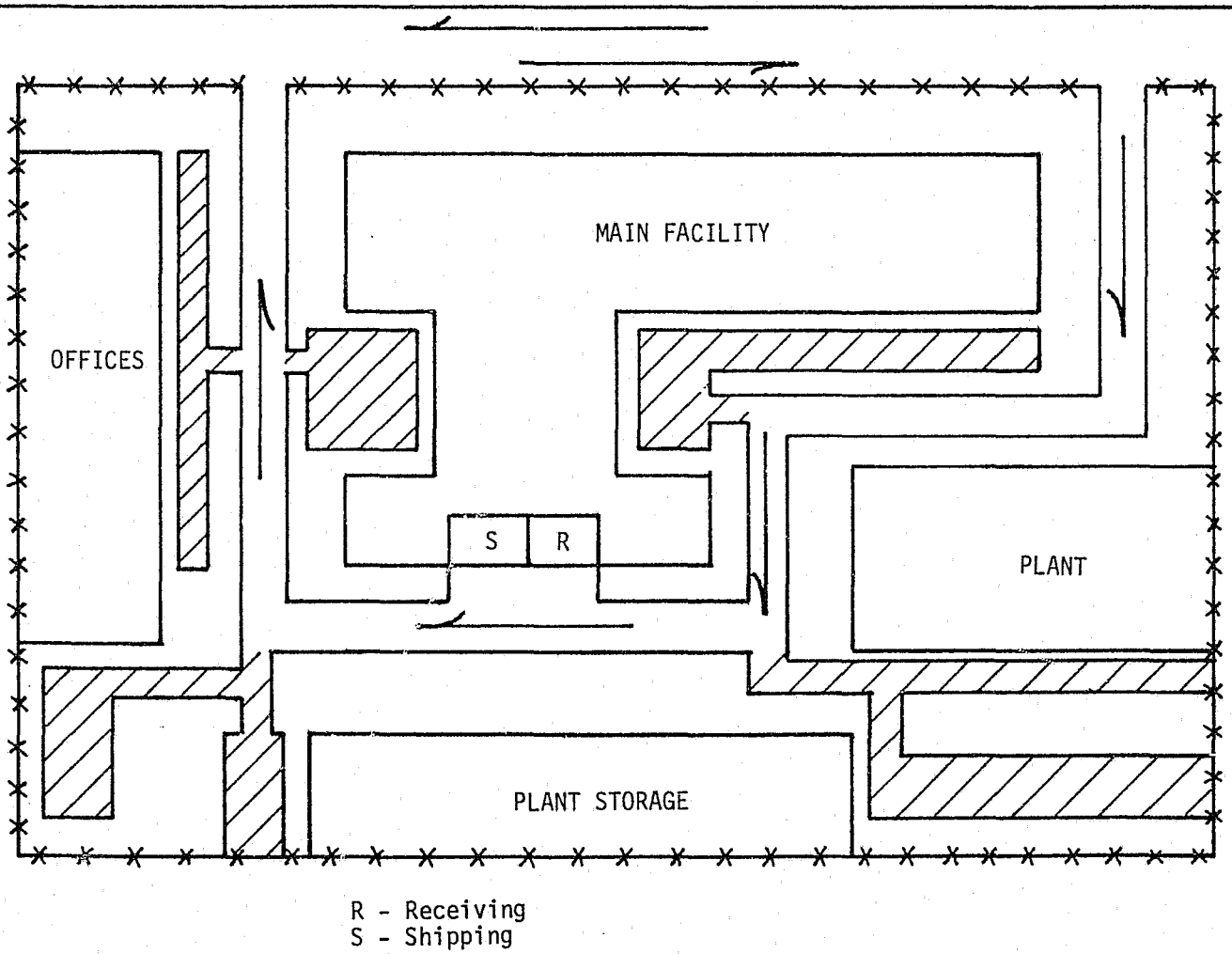


Figure 3-5. Poor Shipping and Receiving Design

- Shipping and receiving functions are performed on each end of a single large dock served by adjoining offices. It is possible to move material and products from shipping to receiving and vice versa at any point in either process. With or without collusion by plant personnel, a delivery truck driver can load items from the shipping dock with low risk of detection.

- There is no provision for surveillance of the shipping and receiving docks by plant personnel. Limited interior surveillance of functional areas is available through windows in the shipping and receiving offices.

- There are check points for vehicles entering and leaving the fenced plant complex, where documentation is timestamped in and out. Seldom is there a physical check of vehicles to compare payloads with weigh bills.

- It is relatively easy for a trucker who illegally loads material not consigned to him to leave the premises without detection.

- The location of shipping and receiving, relative to plant entrances, dictates a long and circuitous flow of traffic, several segments of which are not readily observed. The traffic pattern unduly exposes parking areas, increases the vulnerability of company property along the route, and offers the opportunity for truckers to stop in unobserved areas.

- The juxtaposition of shipping and receiving functions in a single open bay of the plant and adjoining undivided dock favors illegal movement of property from one area to the other.

A more acceptable design for shipping and receiving is utilized in another mid-Atlantic installation (see Figure 3-6).

- Shipping and receiving functions are physically separated and correspond to, and enhance, flow of materials into, through, and out of the plant.

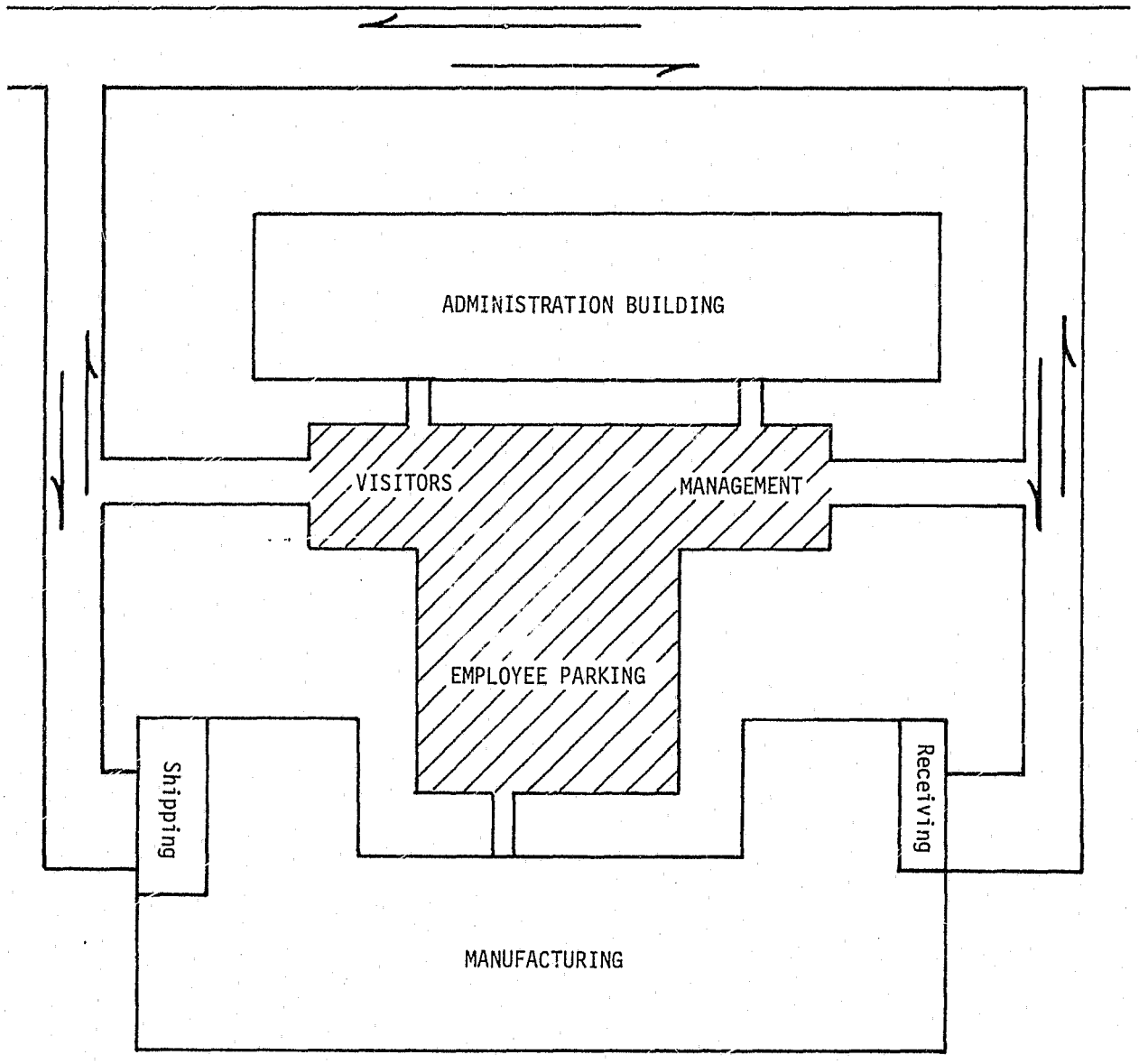


Figure 3-6. Good Shipping and Receiving Design

- A truck must physically move and make a separate approach for a pickup or delivery -- reducing the possibility of not dispensing a scheduled delivery or of making an unscheduled pickup.

- Deliveries and pickups are made through different exits.

- The truck traffic pattern is short, direct, and does not expose other elements of the plant.

- Although there are no security guard check points to control entrance and exit, the docks and internal bays are designed to provide maximum surveillance.

- The internal shipping and receiving bays are physically isolated from the plant bays by attractive but effective barriers with convenient but readily controlled apertures (e.g., counters, gates, and doors).

3.4.6 Coordinating Strategies

No one strategy is likely to be fully effective by itself. Therefore, security engineering entails the incorporation of a family of complementary strategies. A mix of strategies is applicable to deterring theft by employees as well as by outsiders. Many strategies make a contribution to reduction of loss due to both threats.

Just as employee parking lots should not be readily accessible to transients, neither visitor nor employee parking should provide access to vulnerable property. Convenience is an important consideration in the location of parking lots, but it is also important that lot location does not make theft convenient.

It has been said that most commercial loss is suffered at the hands of employees. It may be that a disproportionate portion of the security strategies are directed at the outside threat or, conversely, it may be that employees are assumed to be honest and loyal and, therefore, given insufficient attention as sources of loss. Whatever the reason, greater attention to deterrence of employee theft is needed. Again, the guiding principle is reduction of opportunity, and a mix of complementary strategies is most effective.

Effective accounting and control of valuable, easily-stolen items (such as expensive instruments and tools) is a requisite. Secure central storage with very limited access, inventory, receipts, and strictly supervised issue-and-turn-in policies are self-evident practices. This strategy is frequently not successful because it is not implemented as intended (i.e., the storage is neither secure nor central). In practice, access is not really limited; inventory is not kept up to date; receipts are not required or checked; issue-and-turn-in policies are poorly drawn or not enforced. Above all, management does not review the policies, check the procedures, or inspect the installation and hardware.

Whether the material subject to theft is tools, equipment, material, data, or money, the principles applied are the same: Limit access, establish control, provide surveillance, fix responsibility, and supervise.

Control of interior traffic can be used to limit access and improve informal surveillance in the same way as it is used outside. Marking walkways, posting limited access areas, and arrangement of partitions, doors, gates, and counters contribute to safety as well as security, and the cost can be apportioned accordingly. Furthermore, it is possible to effect control by use of attractive appurtenances, which tend to improve the sense of territoriality and collective responsibility.

Surveillance is also improved, as mentioned elsewhere, by positioning of supervisors, secretaries, and receptionists -- who have been instructed in their surveillance duties. Also mentioned elsewhere is the use of window walls, glass doors, or half-doors, and walls which provide good internal visibility, but not access between groups, functions, and activities.

Training, the subject of a separate section, should be extended to every employee. Indoctrination in responsibility for preventing loss, as well as for the consequences to the organization and guilty persons, are the minimum requirements. Instruction in what to look for and how to detect and deter loss should also be included, as well as training in security precautions and procedures.

Loss due to theft by employees is directly attributable to the stance of management on the issue. By and large, individuals tend to conform to the standards set for, and practiced by, their associates. It is a function of leadership to influence those standards and expectations. To the degree that management tolerates small losses (such as stationery and supplies), management can expect pervasive and expensive losses to otherwise loyal employees.

3.5 Summary

Industry has found that security planning and training pay real dividends in loss prevention and cost reduction. As a result, there is an increasing awareness that a competent security representative should be present from the inception of site planning through installation operation. The practices followed are not complex and most that have been developed are a result of pragmatic proof that they work. The examples provided in this chapter are not exhaustive, but are intended to illustrate how security can be enhanced by observing a few basic concepts. Other commercial practices are described in the specific strategies and concepts presented in Appendices A through D.

CHAPTER 4. NAVY FACILITIES PLANNING CYCLE

4.1 Introduction

4.1.1 Definition

The Navy Facilities Planning Cycle is an integrated, comprehensive, and multidisciplinary process that translates assigned Naval missions into definitions of the facilities needed. Determination of these facility requirements includes quantitative identification of the assets required, comparison with assets available, and initiation of requests to support development or acquisition of assets needed. Responsibility for shore installation planning is assigned to the Naval Facilities Engineering Command by OPNAVINST 11010.1H.

To support these assigned responsibilities, the Naval Facilities Engineering Command (NAVFAC) has developed a Shore Facilities Planning System (SFPS) described in NAVFACINST 11010.44C. The SFPS is supported through separate but integrated automated systems (Master Activity General Information and Control [MAGIC], Category Code Directory [CCD], and Navy Facility Assets Data Base [NFADB]), utilizes the 11000 series of forms, and interfaces with three NAVFAC publications (P-72, P-78, and P-80). It is a quantitative system, permitting comments on a limited number of qualitative factors. Numerous other Navy publications in the 11010 series provide guidance on Shore Facilities Planning and Programming, and establish policies and procedures.

One of the products of the SFPS is an approved OPNAV Form 11000/4 -- Correction of Facilities Deficiencies, which lists individual projects needed to support Naval requirements. This form authorizes preparation of a Form 1391 that, together with a 30-percent design and project cost estimate, becomes the Project Engineering Documentation (PED) for Proposed Military Construction Projects described in NAVFACINST 11010.14L. The 11000/4 is used to support inclusion of the project in the Military Construction Requirements List (MILCON RL).

For purposes of this study, the Navy Facilities Planning Cycle is defined as being initiated with the preparation of the mission or requirement statement, and terminating with the preparation and submission of the Project Engineering Documentation (PED).

4.1.2 Approach

The Navy Facilities Planning Cycle described in Section 4.1.1 can be viewed as three sequential segments, each presenting a different set of opportunities for inclusion of security engineering. These three

segments are the mission or requirements determination and description, the Shore Facility Planning Cycle, and the Project Engineering Documentation. The objectives applicable to each are similar -- that is, requiring inclusion of security engineering concepts and providing guidance on their application -- however, the segments are sufficiently different in structure that the opportunities to achieve these objectives are dissimilar. Therefore, each sequential series of activities is discussed separately, with only the most direct interactions noted.

4.2 Requirements Statements

4.2.1 General

Changes in strategic and technical developments, operational concepts, government policies, human factor relationships, and economic considerations require a continuing reevaluation of Navy mission requirements. This reevaluation forms the basis for the development of revised requirements or mission statements, which are then entered into the Navy Facilities Planning Cycle, and form the basis for preparing OPNAV Form 11000/1.

4.2.2 Discussion

Neither a stated format nor guide has been found for preparing a requirements statement at the "mission" or initiation level, nor has any single source been identified, since requirements for facilities can be identified and initiated at any level from the Congress (environmental impact statement) to the station nonappropriated fund. In any case, the degree to which security engineering considerations should be included depends largely upon the specificity of the requirements statement itself.

It is doubtful that any information that would impact upon the planning cycle will be available at this point in time with the exception of data concerning the mission classification and special physical security requirements. (As previously noted, physical security is considered an included subset of security engineering.) For example, the need for storage facilities for classified data or special security for classified equipment would require consideration in the earliest stages of facilities planning. Therefore, it is felt that known or anticipated special security considerations should be noted at the requirements stage to provide guidance in the development of the facilities plan. This is in accordance with the objectives established for this study and is intuitively acceptable. The policy that requirements statements entering into the Shore Facilities Planning System should include any available information that could impact

upon security and security engineering will help to ensure that any security engineering considerations known to the originator are recorded. The policy will also serve to reinforce security awareness throughout the planning cycle.

4.2.3 Recommendations

It should be an announced Navy policy that statements of requirements to be used as a basis for the development of Naval Shore Facilities construction should include any information concerning any unusual security and security engineering implications or needs.

4.3 Shore Facilities Planning System (SFPS)

4.3.1 General

OPNAVINST 11010.1H establishes the SFPS and its associated policies that integrate the functions of requirement identification, facility planning, asset utilization, programming, and budgeting. In effect, the SFPS serves as the link that joins and coordinates the progressive steps leading to obtaining new or renovated facilities. SFPS can best be envisioned as consisting of three interrelated components: The procedural components (11000 series forms), four automatic data processing (ADP) systems, and various NAVFAC SFPS supportive publications. These three major components are completely integrated in that they are based upon common, interrelated, quantitative factors and definitions. Recorded data are expressed numerically in that the procedures and guidelines established support a quantitative comparison of assets required (e.g., square feet, square yards) and assets available. The single exception is the designation of a set of deficiency codes that can be used as comments to explain ratings given. Within the supporting documentation, there are statements indicating that factors such as safety must be considered in applying the quantitative factors shown -- the inclusion of references to security engineering in these instances appears warranted. However, since it does not appear justifiable to recommend that the basic character of SFPS be changed from its quantitative factor orientation, inclusion of security engineering considerations in the basic system should be in relation to their impact upon the quantitative planning factors provided, and assurance that security engineering has been considered. Recommendations and examples of how this could be accomplished are provided below.

4.3.2 Discussion

There are four procedural components that serve to record the progress of a requirement through the SFPS. These are:

- The Basic Facilities Requirements List (BFRL), OPNAV Form 11000/1, which enumerates by category code the essential facilities required for the activity to perform its mission. The BFRL is an abstract, quantitative statement. It is supported by various studies and analyses such as engineering studies, industrial analyses, and facilities plans. However, the data recorded are expressed in quantitative terms, and gross requirements are developed utilizing pre-established standards.

- The Engineering Evaluation (EE) of Existing Assets, a computerized OPNAV Form 11000/2, which is used to record the results of an EE for onsite, visual inspection and evaluation of each building and structure. The onsite evaluation is accomplished by the cognizant Engineering Field Division (EFD), assisted by activity personnel.

- The Summary of Facility Deficiencies and Excesses, a computerized OPNAV Form 11000/3, is used to provide all echelons of command with information on the extent to which basic facility requirements are fulfilled by existing assets, as well as initial information regarding the extent by which existing assets may exceed an individually categorized requirement.

- The Correction of Facilities Deficiencies, OPNAV Form 11000/4, which is used when the activity has quantified and identified the means for satisfying project deficiencies requiring MILCON funding.

Preparation and use of these forms are described in NAVFACINST 11010.44C (Shore Facilities Planning Manual). Their common denominator is a quantitative statement of assets -- on-hand, excess, or required -- with such statements being made on a numeric basis in terms of an appropriate measurement factor (usually square yards or square feet).

The only provision for entry of a code defining a characteristic of a facility is on OPNAV Form 11000/2, where data element 508 provides for entry of a three-character Deficiency Code (see Table 4-1).

A review of the forms (see Figures 4-1 through 4-4) shows that there is a provision for remarks on OPNAV Form 11000/1. However, guidelines currently provided in OPNAVINST 11010.44C indicate that these are intended to amplify the basis for the units of measurement or basis for estimates.

4.3.3 Recommendations

The procedural components of the SFPS are reports indicating estimates of assets required, or on-hand, stated in quantitative terms. The quantitative data they reflect are developed based upon criteria external to this component. Provision for inclusion of security engineering considerations exists through expansion of the use of the "remarks" section of the 11000/1, designation of additional deficiency codes describing security engineering related subjects, and alteration of OPNAV Form 11000/4 to include a block that, when checked, will certify that security engineering has been considered in developing the project(s) presented. As an alternative to modification of Form 11000/4, a requirement could be established for inclusion of appropriate comments relative to security engineering in Item 33, pending complete implementation of a security engineering program.

Any of these options can be implemented without changing the basic structure of the system. That option calling for an expansion of deficiency codes can be accomplished with relative ease as far as the system is concerned. Care will be required to ensure that deficiencies are, in fact, facilities-related and not the result of operational practices. Such decisions must be based on standard practices and made by trained personnel. Therefore, guidance must be developed regarding application of these codes. Full usage assumes that a definition of security engineering exists and that standards have been defined sufficiently to allow a common understanding of the deficiencies noted. Adoption of these options would also require associated revision (additions) to NAVFACINST 11010.44C to provide instructions on their purpose and use.

- Option 1 -- Include a provision that any unusual security requirements that could influence facilities planning be noted in column 11 -- "remarks" on OPNAV Form 11000/1. To accomplish this, the instructions for use of the remarks column on OPNAV Form 11000/1 should be expanded to include an example of the inclusion of security engineering requirements: "Enter in this column any remarks,

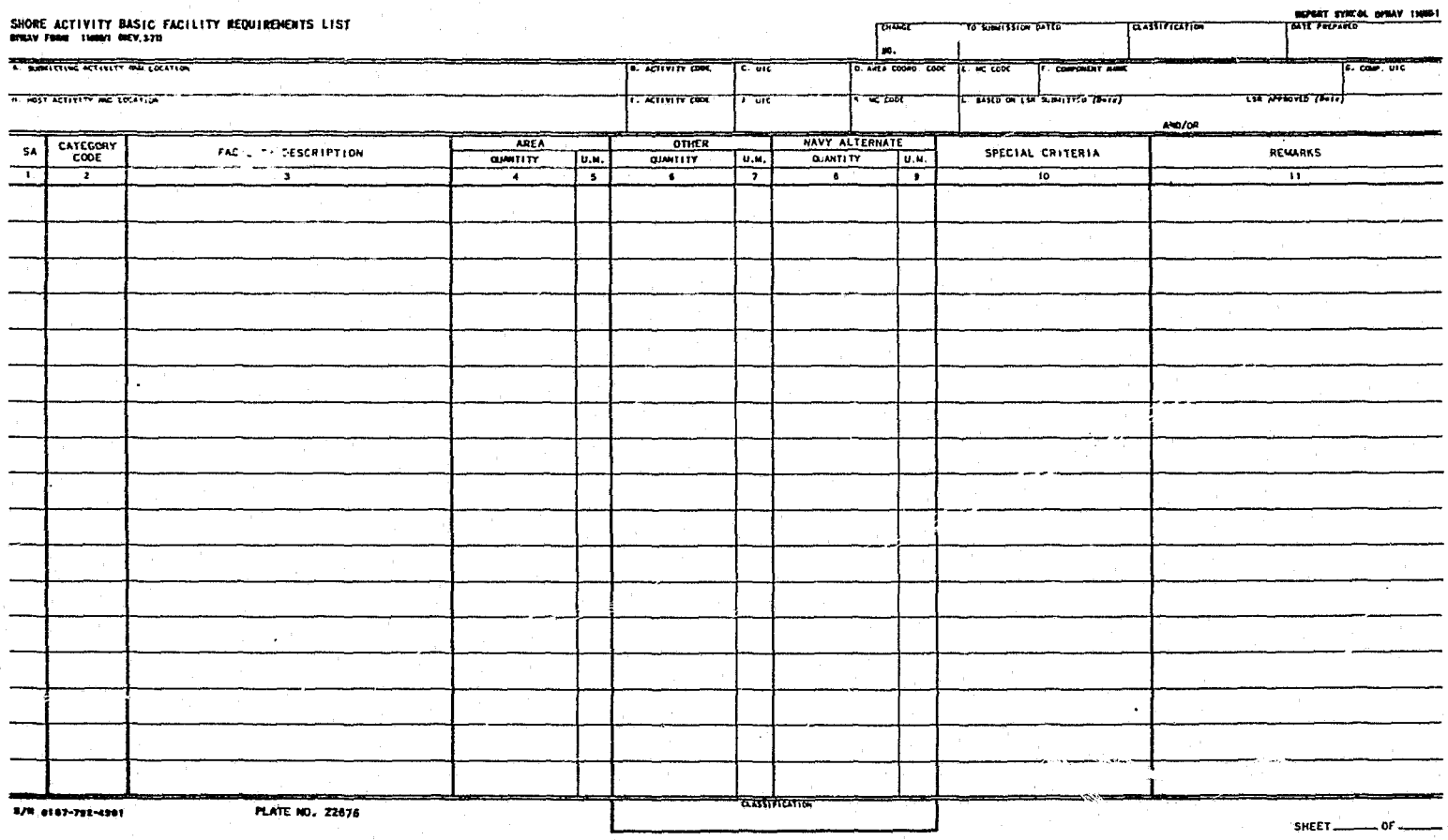
Table 4-1. Three-Character Deficiency Codes

First Character - Deficient Status or Condition Types
(Deficient because of)

A - Physical Condition
B - Functional or Space Criteria
C - Design Criteria
D - Location or Siting Criteria
E - Nonexistence
F - Total Obsolescence or Deterioration
G - Interior Configuration (Bachelor Housing Only)
H - Explosive Load Limit (Magazines)
I - Loading Capacity (Such as Floor Loadings)

Second and Third Characters - Facility Components or Related Items
(Area of deficiency)

01	Heating System	26	Building Interior/ Configuration
02	Ventilation/Exhaust	27	Roof
03	Environmental Control Systems (Air Conditioning, etc.)	28	Soundproofing
04	Plumbing/Piping/Fixtures	29	Waterproofing
05	Fire Deterrent Systems	30	Building or Structure (Total)
06	Fuel System/Piping	31	Fencing
07	Refrigeration System	32	Drainage
08	Elevators/Escalators/and/or Dumbwaiters	33	Landscaping
		34	Stabilization
09	Sewerage, etc.	35	Paved Surfacing
10	Lighting/Fixtures	36	Explosive Quantity Distance
11	Power Capacity	37	Airfield Safety Clearance
12	Wiring/Feeders	38	Pollution Abatement
13	Alarm Systems	39	Excessive Noise
14	Communications	40	OSHA Deficiency
20	Foundation	41	Toilets
21	Slab/Floor Decking	42	Fender Systems
22	Columns	43	Rails/Tracks
23	Walls	44	Cold Iron
24	Roof/Ceiling/Trusses	45	Seismic Design
25	Piling		



SHORE ACTIVITY BASIC FACILITY REQUIREMENTS LIST

OPNAV FORM 11000/1 (REV. 3-73)

REPORT SYMBOL OPNAV 11000-1

CHANGE NO. | TO SUBMISSION DATED | CLASSIFICATION | DATE PREPARED

A. SUBMITTING ACTIVITY AND LOCATION | B. ACTIVITY CODE | C. UIC | D. AREA COORD. CODE | E. MC CODE | F. COMPONENT NAME | G. COMP. UIC

H. HOST ACTIVITY AND LOCATION | I. ACTIVITY CODE | J. UIC | K. MC CODE | L. BASED ON LSR SUBMITTED (Date) | LSR APPROVED (Date)

AND/OR

SA	CATEGORY CODE	FACILITY DESCRIPTION	AREA		OTHER		NAVY ALTERNATE		SPECIAL CRITERIA	REMARKS
			QUANTITY	U.M.	QUANTITY	U.M.	QUANTITY	U.M.		
1	2	3	4	5	6	7	8	9	10	11

S/N 0107-792-4901 PLATE NO. Z2676

CLASSIFICATION

SHEET ____ OF ____

Figure 4-1. OPNAV Form 11000/1 -- Shore Activity Basic Facility Requirements List

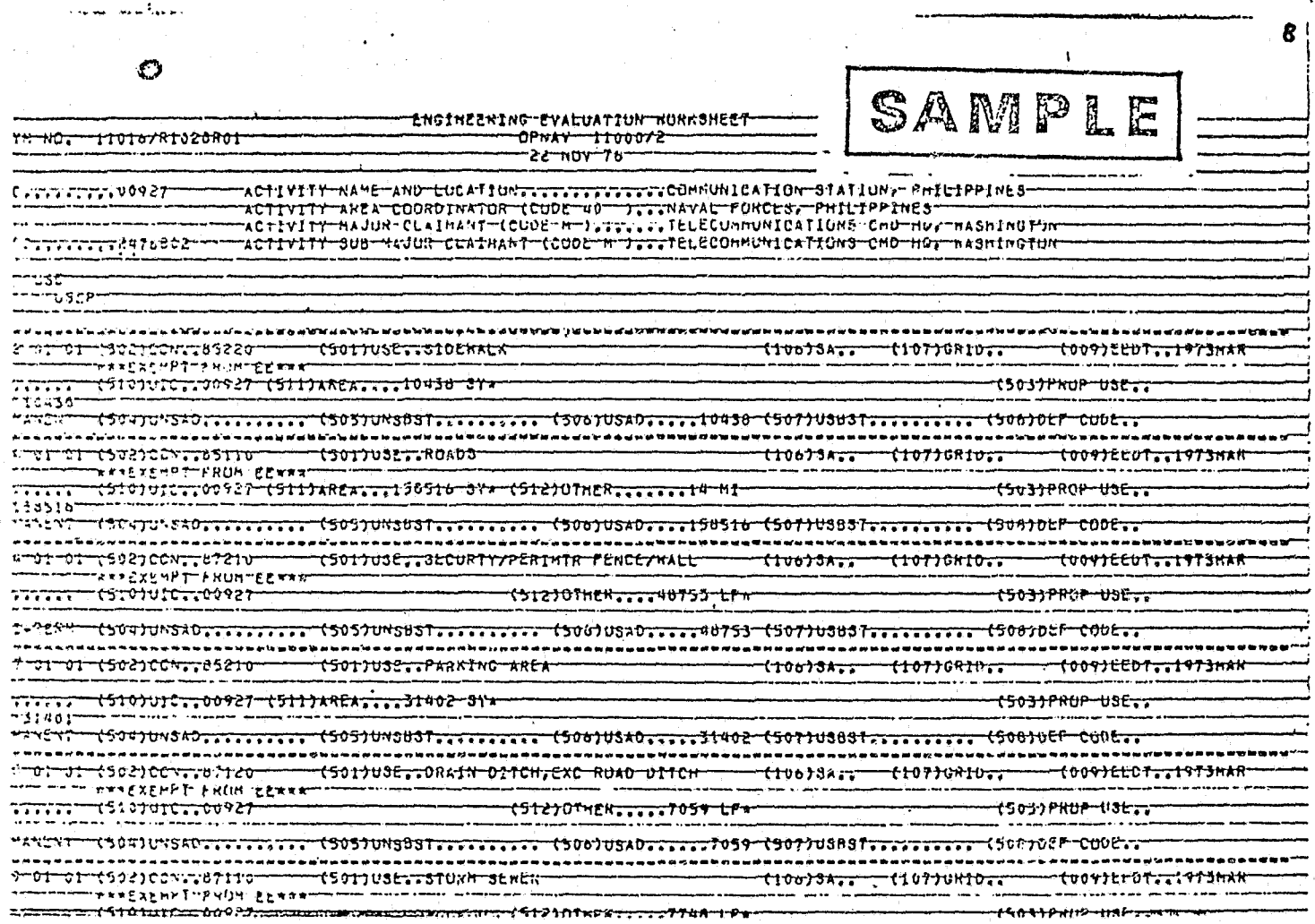


Figure 4-2. OPNAV Form 11000/2 -- Engineering Evaluation Worksheet

FACILITY DEFICIENCIES AND EXCESSES
OPNAV FORM 11000-3 (REV. 6-61)

PERIOD (Check one): ☒ PRE-M-DAY ☐ POST-M-DAY

Reference: Current edition of OPNAVINST 11010.1

CLASSIFICATION STAMP

ACTIVITY AND LOCATION: (illegible) -7

ACTIVITY CODE: 1312-915 | NO OR AREA: 31 | SPONSOR: NAVELSP | FORM STATUS IF OTHER THAN INITIAL ISSUE: ☐ REVISED ☒ CHANGE NO. 1 | PREPARATION DATE: 23 APRIL 19

CATEGORY CODE	FACILITY DESCRIPTION	UNIT OF MEASURE	BASIC REQUIREMENT	EXISTING ASSETS		ASSETS NOT IN INVENTORY	QUANTITY EXCESS	QUANTITY DEFICIENT	SATISFACTION OF DEFICIENCY	
				TOTAL	PORTION SUB-STD.				PROSPECTIVE SOURCE	QUANTITY
1	2	3	4	5	6	7	8	9	10	11
			NAVDET SOUDA BAY							
11-10	RUNWAY	SY	166,670					166,670	NOTE (1-A)	
12-10	TAXIWAY	SY	76,780	22,673				54,107	NOTE (1-A)	
13-20	ACFT PARKING APRON	SY	64,655	16,935	7,835			55,555	PART OF MILCON P-115 NOTE (1-B)	55,1
13-40	ACFT ACCESS APRON	SY	2622	2622						
16-45	LINE VEHICLE PARKING	SY	440	1300			760			

NOTE (1-A) NAVDET SOUDA BAY IS LOCATED ON A NATO MARITIME AIRFIELD, UNDER GREEK COMMAND. THE OPERATIONAL FACILITIES ARE JOINTLY USED BY THE U.S. NAVY AND THE RHAF. THESE JOINT USE FACILITIES SATISFY THE NAVDET RQ

NOTE (1-B) MILCON P-115 WILL PROVIDE 55,555 SY OF ACFT PARKING APRON (CODE 113-20) AN ALSO INCLUDES 61,115 SY OF STABILIZATION TO EXISTING TAXIWAY SHOULDERS

CLASSIFICATION STAMP

SHEET 1 OF ___ SH

Figure 4-3. OPNAV Form 11000/3 -- Facility Deficiencies and Excesses

PROJECT FOR CORRECTION OF FACILITY DEFICIENCY
OPNAV 11000/4 (REV.)

REPORT SYMBOL OPNAV 11000-1C

CLASSIFICATION

PROJECT NO. P –

A. SUBMITTING ACTIVITY NAME AND LOCATION	B. ACTIVITY UIC	C. AREA COORD. CODE	D. CLAIMANT CODE	E. DATE OF LATEST FDR

F. HOST ACTIVITY AND LOCATION	G. HOST UIC	H. COMPONENT NAME	I. COMPONENT UIC

	CATE-GORY CODE	PROJECT TITLE	ALTER-NATE HOST UIC	SPECIAL AREA	SCOPE QUANTITY	SCOPE U.M.	ESTIMATED COST ($000)	EST. COST YEAR	USABLE COMPL. DATE MOS.	USABLE COMPL. DATE Code	% REQ. SATISFIED W	% REQ. SATISFIED W/O	INVESTMENT Prog.	INVESTMENT Master Plan	ECO-NOMIC ANAL-YSIS	E I A	S I T E	MC PRIOR-ITY	CONST/ MISSION CODE	VAL. CODE	21. RELATED PROJECTS
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
J																					
K																					
L																					
M																					
N																					
O																					

CATE-GORY CODE	REQUIRE-MENT BFRL DTD	EXISTING ASSETS DTD (from 11000/2 and 11000/3) ADEQUATE	EXISTING ASSETS SUBSTD	OTHER ASSETS (from 11000/3) FUNDED	OTHER ASSETS NON-NAVY	PREVIOUS PROJECTS QTY	PREVIOUS PROJECTS P-No.	DEFICIENCY	TOTAL THIS PROJECT	DEFICIENCY REMAINING
22	23	24	25	26	27	28	29	30	31	32

33. PROJECT DESCRIPTION/JUSTIFICATION

34. ACTIVITY CERTIFICATION. I certify that this project is required to support activity/mission functions.

Activity Commanding Officer — *Date*

35. EFD CERTIFICATION. This project is supported by SFPS.

EFD Commander/Commanding Officer — *Date*

36. MAJOR CLAIMANT CERTIFICATION. I certify that this project is required to support activity/mission functions.

Major Claimant Representative — *Date*

37. *DO NOT WRITE IN THIS SPACE – FOR NAVFAC USE ONLY.*
This project is authorized for entry into the MILCON R.L.

NAVFAC Authorizing Signature — *Date*

CLASSIFICATION

Figure 4-4. OPNAV Form 11000/4 -- Project for Correction of Facility Deficiency

direct or by note, that are considered pertinent to the facility requirement described such as 'Sensitive material storage required';" "No Criteria Available -- see Note (x)".... (ref. para. ___, OPNAVINST 11010.44C).

- Option 2 -- Expand Deficiency Codes for OPNAV Form 11000/2. It is recommended that the three-character Deficiency Codes (see Table 4-1) be expanded to include security engineering considerations within the present second and third characters identified as 10, 13, 26, 30, 31, and 33, and that additional security engineering related deficiency codes be included (e.g., traffic flow, access control, parking lots).

- Option 3 -- It is recommended that the instructions for preparation of OPNAV Form 11000/4 be revised to include a provision for inclusion of a remark(s) on security engineering in Item 33. Entry of comments here would indicate that consideration has been given to security engineering requirements in development of the data presented. The entry would also highlight any security factors to be considered in the development of project plans.

4.4 SFPS ADP Systems

4.4.1 General

The Naval Facilities Engineering Command has developed, and maintains, four ADP systems that support the SFPS. These are:

- The Master Activity General Information and Control (MAGIC) data base, which is an automated file containing general information on each Navy and Marine Corps shore field activity (e.g., name, location, command relationship, host/tenant relationship, and various codes used by functional data systems). Operational procedures for the MAGIC System are described in NAVFACINST 5400.4.

- The Category Code Directory (CCD), which is an automated file containing the Department of Navy facility category codes; category code nomenclature; and units of measure used for identifying, classifying, and quantifying facility requirements and assets. The file also contains the Investment Category and Maintenance Cost Account Numbers corresponding to each of the facility category codes.

- The Navy Facility Assets Data Base (NFADB), which is an automated file of data on each existing facility (building, structure, utility, and land) owned and/or used by the Navy and Marine Corps. Data are provided on location, type of acquisition, type of construction, cost, size, utilization, and condition. The NFADB is the official record of the Department of Navy Real Property Inventory (RPI). The SFPS uses the NFADB as a record of facility utilization and condition data. Maintenance and operation of the NFADB is described in NFADB Manual, NAVFAC P-78.

Annual reports provided by NFADB are:

- NAVFAC P-77, Inventory of Military Real Property, Navy.

- NAVFAC P-164, Detailed Inventory of Naval Shore Facilities.

- NAVFAC P-319, Statistical Tables of Military Real Property, Navy.

The NFADB maintains data system interface with the MAGIC data base. The MAGIC data base provides standardized information on Navy and Marine Corps activities required by the records and reports produced from the NFADB. The NFADB is also linked by computer to the CCD. The CCD provides standardized facility category nomenclature and units of measure for the records and reports produced from the NFADB.

4.4.2 Discussion

The ADP systems described support the SFPS, and record, manipulate, and report on the assets of the Navy utilizing information provided. No change in the subjective functions or interactions of these systems is recommended. A minor revision will be required to accommodate the additional deficiency codes recommended in Section 4.3.3. However, any more comprehensive approach would require major restructuring or expansion of the system, and is probably not warranted.

4.4.3 Recommendations

It is recommended that the SFPS deficiency code definitions be expanded to include additional Facility Components or Related Items such as those recommended in Section 4.3 and Chapter 6. It is also recommended that general standards or guidance be developed guiding the use of these codes.

4.5 NAVFAC SFPS Publications

4.5.1 General

There are many Navy and NAVFAC publications that must be reviewed if security engineering is to be completely integrated into Navy Facilities planning, programming, and design operations. However, there are four discussed below that provide the basic references and guidance for the Shore Facility Planning System.

Recommendations covering other relevant publications are provided in Chapter 6. The four publications discussed here are:

- NAVFAC P-72 -- Category Codes for Navy Facilities Assets.
- NAVFAC P-78 -- Navy Facilities Assets Data Base Manual.
- NAVFAC P-80 -- Facility Planning Factors Criteria for Navy and Marine Corps Shore Installations.
- NAVFACINST 11010.44C -- Shore Facilities Planning Manual.

As each of these four publications has a specific purpose, so each must be reviewed separately to determine how, and if, security engineering considerations should be incorporated. The objectives desired,

however, can be generalized. That is, quantitative data reflecting the impact of security engineering considerations on planning factors should be identified and users should be provided guidance showing when and how security engineering concepts and principles should be considered.

4.5.1.1 NAVFAC P-72 -- Category Codes for Navy Facilities Assets

This publication establishes the Category Codes/Nomenclature/Units of Measure (CCNs) for identifying, classifying, and quantifying Navy Facility assets, and reports the NAVFAC Investment Categories and Maintenance Cost Accounts so established by the Comptroller of the Navy. The Navy Facilities System is organized to provide an integrated data base for all aspects of facilities planning, programming, budgeting, acquiring, inventorying, maintaining, operating, and disposing of real property. Within these applications, the CCNs are required to identify, classify, and quantify all military real property, facilities owned or controlled by the U. S. Government that have been assigned to the Department of the Navy.

This document establishes a standard series of nomenclatures/codes for Naval Facilities. Even though a review of the categories included reveals none specifically related to any type security (except sentry house), no revision or additions to the document are felt appropriate.

4.5.1.2 NAVFAC P-78 -- Navy Facility Assets Data Base Manual

This publication provides a detailed description of the maintenance operation of the Navy Facility Assets Data Base (NFADB), an automated file of data on each existing facility owned and/or used by the Navy and Marine Corps. Since this is merely an instructional manual and inputs to the NFADB are from the facility categories addressed by the Shore Facilities Planning System (SFPS) discussed previously, no revisions or additions to the document are felt appropriate.

4.5.1.3 NAVFAC P-80 -- Facility Planning Factor Criteria for Navy and Marine Corps Shore Installations

This publication provides facility planning factor criteria and other planning data for use in computing quantitative facility requirements in connection with preparing Basic Facility Requirements Lists

(BFRL), evaluating existing field facilities, and determining specific facilities requirements for shore facilities programs, when applicable as required under the SFPS, for the purpose of attaining a reasonable degree of uniformity and consistency in the computation of facility requirements.

As indicated in this publication under numerous facility planning categories, specific design criteria are contained in NAVFAC Design Manuals. In addition to revisions to P-80 itself, it is, therefore, recommended that security engineering design criteria be included in such a Design Manual and be so indicated within appropriate sections of NAVFAC P-80. Specific recommendations pertaining to such a Design Manual are presented in Chapter 6.

It is through incorporation of security engineering factors in P-80 that the only direct influence on the Shore Facilities Planning System can be accomplished. In addition, the discussion provided describing the various facilities and the ways to apply the planning factors provided a vehicle to direct the user in how to consider and incorporate security engineering-related requirements. Therefore, it is recommended that P-80 be reviewed, in its entirety; that the planning factors provided be revised to include any additional requirements based on security engineering; and that the need for consideration of security engineering be entered.

Examples of such revisions to the P-80 are shown below:*

- Section 5. Architectural and Engineering Standards and Criteria (p.2-6) should be expanded as follows: "... in the process of engineering evaluations at the installation, the question frequently arises as to whether the existing facilities do or do not provide sufficient space to meet customary standards of operating efficiency, safety, security, and habitability..."

*Changes to the P-80 incorporating specific security engineering criteria should be based upon study and experimental data. It is to be expected that these changes will accrue piecemeal as actual plans are reviewed by qualified security engineers and specific experimental data is evaluated establishing the requirement and justification for the change.

- The last sentence of Section 6. Military and Operational Requirements Versus Facility Requirements (pp. 2-6-7) should be expanded as above and read as follows: "....Therefore, the techniques of computing facility requirements and the planning factors contained in this manual should not be interpreted as in any way inhibiting or limiting the authority of a Commanding Officer of an installation to make known his need for additional facilities in order to provide for proper accomplishment of his tasks in the light of established standards of safety, security, habitability, and efficiency."

- Chapter 3. Planning Factor Criteria (p. 3-1), fourth paragraph, should be expanded as follows: "....The allowances specified herein are considered adequate for the efficient performance of the task, while considering the safety, security, and habitability...."

4.5.1.4 NAVFACINST 11010.44C -- Shore Facilities Planning Manual (SFPM)

This document provides the basic instructions for planning Naval Shore facilities by use of the SFPS discussed previously. As indicated in Section 1.A.2, "The planning process is a multidisciplinary effort and gives full consideration to the total environment, including physical characteristics, mission requirements, facility requirements, facility assets and human concerns." Within this statement is the implied understanding that security is a major component; however, as indicated previously, there is no specific mention of security in the planning process. To ensure the most appropriate and cost effective implementation of security concepts, it is necessary that security engineering be considered at the initial facility planning stages. Several methods by which this can be achieved in the OPNAV Form 11000 series were mentioned previously; however, it is recommended that the SFPM be further revised to reflect security engineering. Some additional examples for expansion are:

- Figure 1-3 (p. 1-7) should include Security as one of the criteria to be considered before developing OPNAV Form 11000/1, Basic Facilities Requirements List.

- Section III.C.3.a (p. III-3) should read: "An adequate facility is defined as being capable of supporting its current use without any major modifications on repairs. This means that the facility should be within the limits and restrictions of planning criteria, satisfy structural and mechanical criteria and does not conflict with operational and security engineering requirements or safety restrictions..."

- Changes to several definitions contained in Appendix A (p. A-1) would be appropriate. For example:

  - Adequate (Condition) -- Same as change to Section III.C.3.a.

  - Military Installation Planning -- "The determination of the land and other facilities which will satisfy military operational/security requirements. It includes: Analyses and evaluation of land, water area, and airspace; site selection; determination of buildings, structures and other improvements best suited to satisfy the facility requirements; design of the physical arrangement of the facilities; and assurance of the engineering and construction feasibility of the proposed development."

  - Project -- "A statement of a construction requirement for a facility or group of like facilities in terms of a category code, title, unit of measure, quantity required, estimated cost, description, justification, etc. A project will consist of only those elements necessary to produce a secure/functional entity. It usually has a clearly dominant feature (the principal construction feature) such as a single building or structure, or a group of buildings such as bachelor quarters. Project statements will also be used to identify excess facilities, or for such other identification as may be directed."

4.6 Project Engineering Documentation (PED)

4.6.1 General

Project Engineering Documentation (PED) for Proposed Military Construction Projects includes a supporting Form DD-1391 (see Figure 4-5), and the information developed by a 30-percent design study. PED, which is normally based upon a complete design analysis and developed design concepts, provides design and costing data to support processing and justification of the Military Construction Program to OSD/OMB and the Congress. It includes the following:

- The optimum engineering solution to satisfy the operating requirement at the lowest life-cycle cost.
- A complete and accurate cost estimate that can be explained to reviewing authorities and that will allow construction of the facility within the requested authorization.
- Charts and sketches required to explain and justify the project.

4.6.2 Discussion

It is during the development of the PED that actual costs are first estimated, and the overall designs of the project are first developed. It is also the last time that security engineering concepts affecting site planning, access control, building design, and surveillance and selected cost factors, if any, can be easily included -- once entered into the MILCON RL, revision is difficult, if not impossible.

Therefore, ensuring that security engineering receives consideration by someone qualified to apply the principles and concepts described in the report is critical to achievement of the objectives established. To achieve this, more is required than merely a statement in NAVFACINST 11010.14L, Project Engineering Documentation (PED) for Proposed Military Construction Projects, that security engineering concepts will be applied in developing this documentation. Also required is the development of the expertise necessary to conduct such a review. Recommendations regarding how this should be accomplished are presented in Chapters 5 and 6.

1 COMPONENT	FY 19__ MILITARY CONSTRUCTION PROJECT DATA	2 DATE
3. INSTALLATION AND LOCATION	4. PROJECT TITLE	
5 PROGRAM ELEMENT	6. CATEGORY CODE	7. PROJECT NUMBER	8. PROJECT COST ($000)

9. COST ESTIMATES

ITEM	U/M	QUANTITY	UNIT COST	COST ($000)

10 DESCRIPTION OF PROPOSED CONSTRUCTION

DD FORM 1 DEC 76 1391 — PREVIOUS EDITIONS MAY BE USED INTERNALLY UNTIL EXHAUSTED — PAGE NO

Figure 4-5. Form DD-1391 -- FY19__ Military Construction Project Data (Page 1 of 3)

1. COMPONENT	FY 19_78 MILITARY CONSTRUCTION PROJECT DATA	2. DATE
NAVY		1 FEB 1977

3. INSTALLATION AND LOCATION	4. PROJECT TITLE
COMMANDANT 14TH NAVAL DISTRICT PEARL HARBOR, HAWAII	COMMAND CENTER MODERNIZATION

5. PROGRAM ELEMENT	6. CATEGORY CODE	7. PROJECT NUMBER	8. PROJECT COST ($000)
2 47 51 N	141.41	P-002	4,200

9. COST ESTIMATES

ITEM	U/M	QUANTITY	UNIT COST	COST ($000)
COMMAND CENTER MODERNIZATION	SF	24,775	117.86	2,920
BUILDING ADDITIONS	SF	21,343	113.33	(2,419)
MEZZANINES	SF	3,432	102.56	(352)
BUILT-IN EQUIPMENT	LS	-	-	(104)
RAISED FLOORING	SF	3,654	12.32	(45)
SUPPORTING FACILITIES	-	-	-	871
EMERGENCY POWER SYSTEM	KV	900	351.11	(316)
UNINTERRUPTIBLE POWER SYSTEM	KV	200	2,755	(551)
PARKING	SY	170	23.53	(4)
SUBTOTAL	-	-	-	3,791
CONTINGENCY (5%)	-	-	-	190
ESTIMATED CONTRACT COST	-	-	-	3,981
SUPERVISION, INSPECTION & OVERHEAD (5.5%)	-	-	-	219
TOTAL REQUEST (ROUNDED)	-	-	-	4,200
INSTALLED EQUIP OTHER APPROPRIATIONS	-	-	-	(-)

10. DESCRIPTION OF PROPOSED CONSTRUCTION

Additions and alterations including: increased ceiling height and mezzanine additions; addition for utility areas; providing new freight elevator, air conditioning, security, information distribution and fire protection systems; providing emergency electrical power, and uninterruptible power system.
Air Conditioning - 124 Tons

11. REQUIREMENT

PROJECT: Alterations and additions to the present command center area, in the Commander in Chief, Pacific (CINCPAC) headquarters building, to take advantage of recent developments in equipment and methods for command and control of widely dispersed military forces under diverse situations.
REQUIREMENT: A "situation room" or "war-room" space is required where pertinent intelligence information, situation data, availability and disposition of forces, and other military information can be assembled and made immediately useful to CINCPAC and his staff to properly make decisions to control emergency or wartime situations.
CURRENT SITUATION: The present command center is inadequate in size, function, and habitability to house the computers and displays to support CINCPAC in dynamic decision making. Personnel needed to discharge the full responsibilities of the command center are now scattered throughout the headquarters in ad hoc spaces. Decision making through the use of all available, timely information is not possible. Noise and confusion are brought about by open communications equipment, pnuematic tubes, telephone,

(Continued on DD 1391c)

DD FORM 1 DEC 76 1391 PREVIOUS EDITIONS MAY BE USED INTERNALLY UNTIL EXHAUSTED PAGE NO 40

Figure 4-5. Form DD-1391 -- FY19__ Military Construction Project Data (Page 2 of 3)

1 COMPONENT	FY 1978 MILITARY CONSTRUCTION PROJECT DATA	2 DATE
NAVY		1 FEB 1977

3 INSTALLATION AND LOCATION	
COMMANDANT 14TH NAVAL DISTRICT, PEARL HARBOR, HAWAII	
4. PROJECT TITLE	5. PROJECT NUMBER
COMMAND CENTER MODERNIZATION	P-002

11. REQUIREMENT (Continued)
CURRENT SITUATION: (Continued)
and loudspeaker systems, and use of documents in lieu of display units.
IMPACT IF NOT PROVIDED: Continuation of marginal exploitation of dynamic and near time information systems for effective decision making.

DD FORM 1 DEC 76 1391c — PREVIOUS EDITIONS MAY BE USED INTERNALLY UNTIL EXHAUSTED — PAGE NO 41

Figure 4-5. Form DD-1391 -- FY19__ Military Construction Project Data
(Page 3 of 3)

4.6.3 Recommendations

It is herein recommended that NAVFACINST 11010.14L specify a requirement that security engineering requirements be considered in the preparation of any PED, as well as in the development of Facility Studies at the local level. Until the Navy has trained individuals capable of accomplishing this function, it should require that it be done as part of any contract negotiated for facility design to architectural engineering firms.

CHAPTER 5. PROGRAM CONSIDERATIONS

5.1 Introduction

There is currently no single discipline or compilation of data that can be pointed to and termed security engineering. There is, however, a set of concepts and application strategies that are proving to be effective in reducing crime, as well as a small but growing number of practitioners who are applying these concepts in facilities design, construction, and renovation. As a result, introducing security engineering into the Naval establishment requires more than simply including a requirement that security engineering principles be applied. It requires development of a series of guidelines as to what security engineering is and how it should be applied, as well as for the training of those individuals to be responsible for the program and its implementation. Responsibilities must be assigned, and directives must be issued to include security engineering guidance and requirements. While the development of such a program for the Navy does not fall within the scope of this report, information has been obtained that may prove helpful in the development of such a program by the responsible headquarters or agency. That information is provided by topic in this chapter, as well as recommendations as to actions that should be taken in the development of a Navy program.

5.2 Supporting Publications

A prerequisite to the implementation of any new area of expertise is the existence of publications or documents in which it is described. In the Navy, instructions and definitions on subjects comparable to security engineering are published in Design Manuals. NAVFAC DM1, Architecture contains material that provides guidance in the area of security engineering application, and changes to this manual applicable to specific areas of interest have been published. For example, Change 1, dated March 1976, contains design concepts applicable to compliance with requirements for the physically handicapped.

It is recommended that guidance concerning when to consider security engineering be incorporated throughout the basic manual. For example, Chapter 2 (Concept Design -- General and Special Design Considerations) of DM1 presently contains numerous sections in which physical security considerations could and should be implemented. NAVFAC Requirements and NAVFAC Objective (p. 1-2-3) are prime targets. These subsections could be revised to read as follows:

b. NAVFAC Requirements. NAVFAC requires the architect-engineer to apply human engineering principles and criteria throughout the design of the project. The following list some, but not all, of the areas of concern.

(1) Site Development. The architect-engineer should concern himself with environmental factors, weather, and climate aspects, acoustic noise if applicable, safe and efficient walkways, parking, and drives, and other exterior factors where they relate to human and security engineering emphasizing the physical security of people and property.

(2) Building. Illumination levels will be designed according to specific task and security requirements...

(3) Interiors and Equipment. Human engineering criteria shall be applied to room layouts, stairs, ramps, ladders, and work areas with emphasis on the physical security of people and property ... Colors shall be chosen for psychological, safety, security, emotional, fatigue, and other governing factors.

c. NAVFAC Objective. Military systems, equipment and facilities shall be designed to provide work environments which foster effective procedures, work patterns, personal safety, and personal and property security, and which minimize discomfort, distraction, and any other factors which degrade human performance or increase error.

The foregoing are presented as examples only. The entire manual should be expanded to include security engineering at its next revision. In addition, a change providing specific design guidance should be prepared and published as soon as possible. Data provided in this report are deemed supportive of such an initial effort, and could serve as an initial introduction to the principles. Completely adequate coverage will require preparation of an expanded DM1 incorporating more detailed guidance.

While DM1 has been identified as a primary means for provision of security engineering guidance, there are many other manuals in which security engineering should be incorporated. Identification of such manuals and development of recommended additions and revisions should be accomplished. For example, the joint manual on "Site Planning" should highlight security engineering requirements, and its revision represents a logical step in the implementation process.

5.3 Threat Analysis

A basic assumption throughout this study has been that application of security engineering concepts is cost-effective (i.e., that the dollar savings due to decreased loss will far exceed the costs of the improvements or modifications). There is little question that this is true at the design stage; with the possible exception of better grade building materials or incorporation of security hardware, there is normally little additional cost associated with changes at this stage. Even at this stage, however, there are trade-offs between costs and requirements, and security, unless strongly represented, is often one of the losses.

In later stages, particularly in renovation where incorporation or observance of security engineering is an identifiable cost, justification of such expenditures may well require "cost reduction" identification. As noted previously, security engineering concepts are being applied in the commercial area based upon a belief that they are cost reducing. There are, however, little real data to prove this. One estimate of Navy security-related losses was stated to be possibly as high as $100,000,000 a year. Little or no hard data seem to be available to support this estimate.

A pragmatic assessment of what is needed for security engineering to be applied in the Navy leads to the conclusion that it will be largely dependent upon the savings which can be achieved (i.e., the cost/benefit ratio).

The classical development of countermeasures follows the definition of the threat to be countered. This holds true in CPTED theory -- the first step to be taken is an analysis of crime patterns to define the problem after which specific strategies can be developed. In the application of security engineering concepts, a knowledge of the area and extent of losses is required. Where losses are small, major renovation for security is not justified. Therefore, to determine which security engineering strategies are applicable to Naval Shore Facilities, it is recommended that a study be conducted at specific Navy facilities to determine the extent of security-related losses being experienced, as well as to determine the specific areas in which they occur.

5.4 Training

5.4.1 General

The Navy has a well-defined training program that provides for training at both the general and specialist level. This training is complemented by the MOS award system that identifies those individuals who are considered specialists in their field. This approach is duplicated in commercial practice, although the recognition of individual capabilities is at a less formal level.

Training in security engineering in the private and public sectors has received emphasis only in the last few years. Three recent examples of such training courses are: (a) The "Crime Prevention Through Environmental Design" course, conducted at the Urbana campus of the University of Illinois; (b) a "Comprehensive Assets Security Course," held by the American Society for Industrial Security in Old Town, Alexandria, Virginia; and (c) a "Security Management Functions and Policies Course 520," held by a large corporation.

Each of these has differed in course content and, to some extent, in course objectives. However, as a composite, they indicate the current approach to training in the security engineering and related (CPTED and Security) areas.

5.4.1.1 CPTED Course

The University of Illinois CPTED course was initiated during the fall semester of 1975 as a multidisciplinary course primarily intended for graduate and advanced undergraduate students in the design and social science fields. The course was sponsored by the Department of Art and Design, Industrial Design option, offering 3 hours -3/4 units of academic credit. Class meetings were held once each week for two hours per session.

During the spring semester of 1976, the Departments of Architecture and Industrial Design joined as cosponsors of the CPTED course. The Department of Architecture also provided a quarter-time teaching assistantship to support class preparation activities.

During its first year, 36 students successfully completed the CPTED course. These students represent diverse professional disciplines, including architecture, finance, graphic design, industrial design, landscape architecture, psychology, and urban planning. Many of these students have already graduated from the University and are engaged in professional practice.

The purpose of the course is to instill in future professionals an awareness of how their activities can promote crime prevention objectives. To this end, such a course can provide a forum where diverse professional perspectives and interests can be explored, concepts can be developed, and information can be disseminated.

Since CPTED is by nature a process that cuts across many professions and interest groups, the multidisciplinary emphasis of the course is of fundamental importance. Summarized briefly, key objectives of the CPTED course are to:

- Provide a general overview of national crime patterns, trends, and intervention approaches to familiarize persons with little or no experience in criminology/law enforcement with basic problems, procedures, and literature/data.

- Review selected environment- and site-specific case studies to illustrate various crime intervention planning approaches, priorities, problems, and results.

- Provide a forum for the exchange of diverse viewpoints on subjects related to crime prevention approaches, priorities, impacts, and implications. (This is accomplished through guest speaker appearances and informal large and small group discussions.)

- Provide incentives and assistance that will encourage each student to identify a crime/environment problem that can be impacted by members of his profession, and consider how an appropriate action plan might be initiated to address the situation. In short, each student is required to demonstrate an awareness of CPTED principles through work on an individual project.

5.4.1.2 Assets Security Course

The Comprehensive Assets Security Course is one of three held periodically by the Professional Development, Education, and Training Committee of the American Society for Industrial Security (ASIS). The other two are an Advanced Security Management Program, and a Professional Certification Review. As its name implies, the Comprehensive Course covers many aspects of security in its 5-day session. Sessions held are noted below, with those on security presently incorporating some discussion on security engineering matters.

- Security Vulnerability.

- Security Surveys.

- Systems in Security.

- Guard Operations and Functions.

- Strikes and Labor Disturbances.

- General Security Management.
- Countermeasures Workshop.
- Investigations.
- Dealing with Terrorism.
- EDP and Computer Operations.
- Protecting Proprietary Information.

5.4.1.3 Security Management Course

The Security Management Course is a 3-day course presented by a major corporation's Security Department and outside consultants. It was designed to better train first-line supervisors and professionals responsible for security and loss prevention. The course stresses skills necessary to establish and conduct a cost-effective security program, in recognition of the increasing exposure of all corporate facilities to losses through theft, as well as the need to provide less costly alternatives for security. The course is open to auditors and accounting personnel, warehouse and office managers, and personnel relations employees, as well as individuals involved with basic security or loss prevention programs. While not a specified subject, security engineering concepts are discussed and presented throughout the course. The course objectives and course outline are shown below:

Course Objectives

Following this course, the participant will have:

- Sufficient background and understanding of the theory and techniques of security management for planning, managing, and performing in a responsible security position. This course is designed primarily for the individual who has responsibility for a security program but has had little formal training. In addition, it will be beneficial to those responsible for asset protection or who have an interest in loss prevention.
- A basic knowledge and understanding of the requirements for, cost of, and effective utilization of plant protection personnel.

- A knowledge of the basic principles of detection and prevention of theft and pilferage.

- Acquired an adequate knowledge of alarm systems to be able to determine whether any economic benefit can be obtained locally.

- A knowledge of specific areas where further preventative effort should be expended.

5.4.2 Discussion

As in the private sector, the Navy should have two levels of security engineering training. One, at the graduate level, should be an applications-type course for architects or engineers responsible for the design and construction of Navy facilities. It should include a discussion of the basis for the concepts presented, and practical experience in their application. At the conclusion of the course, a prefix or suffix could be awarded. It is suggested that responsibility for such a course be that of the School at Port Hueneme.

The second need for training is at the level of that described in Section 5.4.1.3. Within the Navy, such training could be both a short familiarization course and a block of instruction in career and management courses. While much data are available for such courses from the private sector, it can be logically assumed that class interaction would also provide valuable information.

5.4.3 Recommendations

For the Navy to achieve the required security engineering expertise, it is recommended that training courses be developed as follows:

- A block of instruction of not less than 8 hours on security engineering be developed for inclusion in career and management courses. The period recommended is exclusive of instruction on physical security, even though the instruction might be integrated.

- A block of instruction or separate refresher course of approximately 40 hours be developed for individuals responsible for security engineering applications (i.e., architects, construction engineers, security planners).

- Security engineering short courses offered by professional societies and universities should be utilized to broaden the background of appropriate planning and design personnel.

5.5 Summary

Effective observance of security engineering in Navy Facilities Planning and construction will require establishment of an integrated program providing for definition of standards, guidelines, and training of personnel. Current Navy and commercial practices provide firm guidance as to how such a program should be developed and implemented.

CHAPTER 6. SUMMARY OF RECOMMENDATIONS

6.1 Introduction

The recommendations made in this chapter are based upon Navy documents reviewed and conferences held during the course of this study. They also represent the opinions of practitioners in the (admittedly new) field of Crime Prevention Through Environmental Design (CPTED) and its included area of security engineering. Taken as a whole, the recommendations are designed to ensure development of security engineering awareness throughout the Navy, and incorporation of security engineering concepts into the Navy Facilities Planning Cycle.

The program outlined is of necessity comprehensive since in recognizing the inherent benefits, both financial and operational, which can be achieved through the application of security engineering, the Navy is acting as a pioneer in the field. This is not to imply that security is not a current concern, simply that the focus of major ongoing efforts is on different aspects of security. In the public sector, the major study effort, CPTED, is concentrating on crimes of violence, and considers the complete field of social and behavioral psychology as well as physical design concepts and strategies. In the military, much emphasis is placed on physical security, particularly as it applies to specific threats and sensitive installations. The direct interaction between developments in these areas and security engineering should be recognized, and security engineering design concepts continually reviewed to ensure that they are compatible with the latest developments in these fields.

Recommendations are grouped by area of responsibility as much as appeared practical. As in any such program, some will take longer to accomplish than others, with initiation of effort being dependent upon command approval of this report and publication of implementing directives. An initial attempt to propose a time phasing for program initiation was abandoned when it was determined that insufficient data on the lead times necessary for action within the Navy were available without further investigation and that such research was not within the scope of the study.

6.2 Navy Facilities Planning Cycle

Recommendations concerning the Navy Facilities Planning Cycle are intended to foster awareness of the need to consider security engineering in the development of construction projects, to ensure

consideration of quantitative requirements based upon security engineering needs, and to provide a record that these have been accomplished. To achieve these objectives, the following recommendations are proposed:

- It should be an announced Navy policy that statements of requirements to be used as a basis for the development of Naval Shore Facilities construction include any information available concerning security and security engineering implications or needs.

- Security engineering should be considered throughout the Shore Facilities Planning System. Provision exists through expansion of the use of the "remarks" section of OPNAV Form 11000/1 to require comment on any security implications known; designation of additional three-character deficiency codes for use with OPNAV Form 11000/3 to describe security engineering related subjects; and alteration of OPNAV Form 11000/4 to include a block that, when checked, will certify that security engineering has been considered in developing the project(s) presented. As an alternative to modification of Form 11000/4, a requirement could be established for inclusion of appropriate comments relative to security engineering in Item 33, pending complete implementation of a security engineering program.

- Of the four ADP systems that the Navy Facilities Engineering Command maintains to support the SFPS, no change in the subjective functions or interactions of these systems is recommended, although a minor revision will be required to accommodate the additional deficiency codes recommended. It is, therefore, recommended that the SFPS deficiency code definitions be expanded to include additional Facility Components or Related Items and that general standards or guidance be developed guiding the use of these codes.

- There are many Navy and NAVFAC publications that must be reviewed if security engineering is to be completely integrated into Navy Facilities planning, programming, and design operations.

However, there are four that provide the basic references and guidance for the SFPS (i.e., NAVFAC P-72 -- Category Codes for Navy Facilities Assets; NAVFAC P-78 -- Navy Facilities Assets Data Base Manual; NAVFAC P-80 -- Facility Planning Factors Criteria for Navy and Marine Corps Shore Installations; NAVFACINST 11010.44C -- Shore Facilities Planning Manual).

- NAVFAC P-72 -- No revisions or additions to the document are felt appropriate.

- NAVFAC P-78 -- No revisions or additions to the document are felt appropriate.

- NAVFAC P-80 -- It is through incorporation of security engineering considerations and factors in P-80 that the only direct influence on the SFPS can be accomplished. Therefore, it is recommended that the P-80 be reviewed in its entirety and that reference to the need for considering security engineering be entered. Planning factors provided should be reviewed and revised as appropriate. As indicated in this publication under numerous facility planning categories, specific design criteria are contained in NAVFAC Design Manuals. Therefore, it is further recommended that security engineering design criteria be included in such a Design Manual, and be so indicated within appropriate sections of NAVFAC P-80.

- NAVFACINST 11010.44C -- Since this document provides the basic instructions for planning Naval Shore Facilities use of the SFPS, it is recommended that the NAVACINST 11010.44C be further revised to reflect security engineering.

- It is recommended that NAVFACINST 11010.14L, Project Engineering Documentation, specify a requirement that security engineering requirements be considered in the preparation of any PED, as well as in the development of Facilities studies at the local level.

6.3 Training

Development of knowledgeable practitioners in the field of security engineering requires both formalized and on-the-job training for those individuals who will be responsible for the design and construction of new facilities and the renovation of old ones. Proper exploitation of the benefits provided by facilities constructed to reflect security engineering concepts requires a general awareness of security engineering concepts and considerations. Therefore, training courses should be developed for both categories of personnel. To accomplish this, the following recommendations are proposed:

- A Block of instruction of not less than 8 hours on security engineering should be developed for inclusion in career and management courses. The 8 hours recommended is exclusive of instruction on physical security, even though the instruction might be integrated.

- A block of instruction or separate refresher course of approximately 40 hours be developed for individuals responsible for security engineering applications (i.e., architects, construction engineers, security planners).

- Instruction on security engineering should include as an introduction, background data on developments in the related areas of physical security and Crime Prevention Through Environmental Design (CPTED) to show their interrelation with security engineering.

6.4 Threat Analysis

The security engineering concepts and practices outlined in this report are based upon practices in the field and widely recognized threats. They are intuitively satisfying and have proven effective whenever evaluated. An attempt has been made to present those with wide application, and with minimal cost (at least, if incorporated at the design stage). Nevertheless, certain strategies will have to compete for available funds with other worthy projects. To allow tailoring of security engineering strategies, and to provide some realistic measure of possible cost savings, the following recommendation is proposed:

- A study or studies to be made at specific Navy facilities to determine the losses being experienced due to theft, and the specific areas in which these losses occur. As a part of this study, or as a logical next step, security engineering strategies should be implemented and the changes in loss volume and patterns determined. A concurrent review should be made of the planning factors contained in P-80 to determine if revision is indicated.

APPENDIX A

Security Engineering Concepts Applicable to an Installation

1. INTRODUCTION

The security planner for the installation should be primarily concerned with influencing spatial relationships, perimeter control, and traffic flow plans so as to enhance security. To do so, he must participate in the planning for the installation and be cognizant of the impact upon security of the decisions reached. He must identify the vulnerabilities of the installation, the operational characteristics of the missions to be performed, and carefully chart those activities and resources which will impact upon security. It is obvious that it is at this stage that proper security engineering can be most effectively (and inexpensively) incorporated. This is as true today as in 1971 when M. Liechenstein in his Design for Security wrote:

> "The key to economical security design lies in security planning before construction, ... and in sharing portions of the security system among other uses.
>
> The most obvious opportunity for multifunction usage is in providing fire, burglary, robbery, and utility protection, all of which have some commonality of goals, i.e., protection of property and/or personal safety."

2. SECURITY ENGINEERING CONSIDERATIONS

2.1 Site Selection

Although it is probable that security engineering criteria will never be the deciding factor for facility site selection, the security planner should become involved in the planning cycle as early as possible. If he can become involved at the site selection stage, it will provide him both an opportunity to point out security characteristics of sites being considered and to become familiar with the operations being planned. In the course of the selection process, he should discuss security with the other members of the team and indoctrinate them as to security concepts.

His security planning during this period should be at the detail level corresponding to that of other members of the team. However, it should include, at a minimum, considerations of natural barriers, both internal and external to the site, site access points, external traffic flow, the potential threat posed by surrounding communities, and the local crime prevention situation.

2.2 Site Planning

To successfully influence the site plan, the security planner must actively participate in the initial stages when the first functional

grouping of activities occurs. In general terms, facilities utilized by distinct classes of personnel should be grouped, traffic from offsite should be routed to and from the facilities used by as short a route as possible, and maximum use should be made of surveillance opportunities provided by facilities manned on a 24-hour basis. Specific strategies are discussed later, but following these general guidelines, hospitals and commissaries would be near residential areas, and both would be near an access point. Shipping and receiving facilities would be grouped near a separate gate, and sensitive material storage areas might be grouped near an operation, such as a fire station, manned at all times. Another consideration would be to group offices occupied only during normal duty hours so they could be easily patrolled and intruders would be conspicuous.

A possible approach is to prepare an occupancy and traffic flow plan showing conditions each four hours through the day. Use of such simple diagrams will serve to highlight traffic flow and surveillance problems, particularly if the locations of sensitive security items and operations are included. Some specific items to be considered are listed below.

2.2.1 Topography

The security engineer should make maximum use of existing conditions to enhance security and, where the natural or existent environment is to be modified, should ensure that security is enhanced not degraded. Open terrain improves visibility and surveillance; steep, rough terrain limits it. Both improved surveillance and access control can be achieved by grading, much of which will occur as a function of construction. Low mounds act as barriers and do not impede surveillance. Obstructions to visibility on or near the property, in the form of woods and undergrowth, may be either desirable or undesirable. Where woods constitute a covered avenue of approach or hiding place, they should be cleared or contained by a manmade barrier. Where they are a barrier, the barrier can be enhanced by the use of fencing. A body of water, like an adjoining woods, is both a barrier and an avenue of approach to be considered in the plan. To the degree that it requires a readily observable crossing, a body of water is an excellent barrier. To the extent that the water is an avenue and a point of access, it is a weak link in the security chain. The security engineer should devise strategies to improve natural and formal surveillance and to restrict potential landing points if such access will pose a threat to his installation.

2.2.2 Perimeter Control

Some type of perimeter control is common to most installations. Depending upon the size and security requirements, this control may consist of commercial type fences, natural barriers, or elaborate

barriers and associated sensors. The security planner should strive to make the maximum use of natural deterrents and to maintain a common level of security at all points. Specific external threats should be recognized by specifically developed deterrents. For example, an area adjacent to a school should be designed to either channel or prevent intrusion by children. Use of a barrier attractive to children, such as a woods or stream, should be avoided. Mounds of earth and low-growing, dense shrubbery would probably be effective. Barriers such as rivers, streams, ravines, buildings, and forests must be considered as avenues of approach as well as barriers and evaluated based upon the degree of security desired.

2.2.3 Access

Access is a broad criterion applicable to the site, specialized areas, facilities, buildings, and activities within the site. The objective is to limit and control access within the limits imposed by efficient operations, which implies provision for ready access by authorized persons at authorized times. Good security engineering strategy will limit -- to the minimum consistent with efficient operation of the facility -- the number of points through which personnel and vehicles can enter. Flexibility is provided by including additional points of entry that are normally closed but can be opened for special purposes.

Access to specific areas (such as dependent housing, medical facilities, command post) are controlled by their location and traffic patterns within the installation. Access can be deliberately sacrificed to achieve greater surveillance. These kinds of judgments are made with the knowledge of the conditions of the time and place, recognizing that over the life of the installation those conditions and even the use to which the facility is put will change.

2.2.4 Traffic

Although sometimes construed to be a subset of access, the control, pattern, and flow of traffic is sufficiently important to security planning that it warrants separate discussion.

In the interest of efficiency, as well as security, the shortest, most direct route is the best. Long and circuitous routes increase exposure and provide opportunities for on- and off-loading without detection. Therefore, the strategy is to lay out or change routes so that they are short, direct, and continuously under some form of surveillance.

Normally, pickup and delivery vehicles should be routed directly, by the shortest route, from the point of entry to the point of delivery or pickup. Moreover, access points, building arrangement, and road

layout should be planned with this objective in mind. Minimizing points of entry and minimizing distances from point of entry to all destinations within the installation will require some design compromises.

2.2.5 Grouping of Facilities

Considerations relating to the arrangement of buildings, facilities, and activities within the installation are affected by the mission, size and shape of area, type of facility, number and size of buildings, and a myriad of other factors.

Ideally, buildings are grouped by function: Command and control, operations, supply, base maintenance, and personnel support (such as housing, medical, dining, recreation, chapel, exchange).

Parking facilities will be required at work, recreation, and housing facilities. Parking lots are vulnerable areas and should, therefore, be placed where surveillance exists in the normal course of activity in adjoining areas. Lighting and patrolling are added as required.

Deadend streets should be considered in housing and other areas to control traffic and limit access. Removable barricades can provide control to create deadend streets, as well as provide flexibility for exceptional traffic requirements.

Delivery and pickup sites are points whose vulnerability should be reduced by a combination of techniques, including short direct routes, physical separation, and planned surveillance. Scrap and salvage yards, trash pickup and deposit points, shipping and receiving functions, food delivery, and receipt of medical and other supplies not directly related to the principal mission of the installation are in the high vulnerability category. All are subject to the same strategies to minimize dispersion and opportunities for unobserved operations.

Open spaces between buildings and particularly between groups of buildings grouped by activity are needed to provide good fields of view, a sense of responsibility and proprietorship on the part of the users or occupants, and ease in identification of strangers arriving and departing. One hundred feet or more around major buildings is considered an absolute minimum.

2.2.6 Surveillance

The plan for surveillance should consider not only programmed and scheduled observation and inspection by guards and others having surveillance as an assigned function, but also intermittent informal surveillance. The formal portion of the surveillance plan provides manned

gates, guard posts, and 24-hour coverage of critical areas (such as computer rooms, classified areas, police stations). Although unscheduled, the informal portion of the plan is deliberately planned to ensure that vulnerable areas, property, and activity are within the clear view of persons directly related to the activity and also others who may have no relation to (or responsibility for) it. The strategy for informal surveillance is to provide a field of view overlooking vulnerable areas and to ensure a minimum density of activity and personnel presence in the area during the most vulnerable period. There are numerous opportunities to substitute informal for formal surveillance without loss of effectiveness and at a cost saving.

Open spaces and spatial relationships -- as well as windows, walks, and other features that place people in position and able to observe -- are an integral part of the surveillance plan. Within an industrial installation, for example, a computer complex manned 24-hours a day could be located to enhance surveillance of a parking area, or an all-night cafeteria could be located so that its patrons would pass rooms or buildings where sensitive items were stored. Lighting required to illuminate walks and parking areas could serve a double function if it also illuminated vulnerable building entry points. In a similar fashion the location of windows to overlook a shipping dock makes possible observation of the dock by persons not working in the shipping department. In each case, the possibility of observation acts as a deterrent to criminal activity.

3. SECURITY ENGINEERING STRATEGIES

3.1 General

As in most real-world situations, designing for security at the installation level involves a series of compromises. The installation's primary purpose is to support accomplishment of a mission, or group of missions, and in some cases security considerations will be overridden. In most cases, however, enhanced security can be achieved with no mission degradation, simply by manipulating spatial relationships or modifying facilities design. The major objective of the security planner is to achieve the latter at all times, and where security considerations conflict with other considerations, he should be prepared to support his recommendations with data on projected cost savings and enhanced security. Specific strategies that he should consider in developing his recommendations are noted below.

3.2 Perimeter Control

Security engineering can be viewed as the establishment of a series of deterrents to inhibit criminal activity. The first of this series is established at the perimeter, which should be viewed both as a means of limiting access and as a screening point. Security engineering

recognizes that the majority of losses, dollarwise, are due to individuals who are authorized access to the area of loss. It also recognizes, however, that reducing opportunity by reducing exposure will reduce loss. The perimeter and its access points should be designed with both points in mind. Specific strategies that should be applied are to:

- Establish access points as close as possible to the areas to be served to minimize unnecessary travel on the installation. Access points servicing normal-hour functions only should then be closed during nonduty hours to simplify surveillance.

- Utilize low mounds and shrubbery to restrict installation entry and to enhance surveillance.

- Segregate commercial and normal traffic entry points to assist in shipping and receiving control.

- Provide nighttime illumination of boundary areas shining towards the exterior of the installation.

- Protect or secure openings such as culverts, tunnels, or ravines which could provide avenues of entry to the installation.

- Ensure that access points are well-lighted at night and that secured entrances are adequately equipped with locking devices.

3.3 Functions Grouping

Security is simplified if facilities having common security requirements are grouped. Residential areas, office buildings, repair facilities, and public support functions all have different types of users, different hours of use, and different types of security problems. By grouping them, common security procedures can be observed, and access and traffic patterns can be planned. Some specific strategies to enhance security at lower costs are to:

- Group office buildings or support facilities so that a minimum number of access points need be maintained during off-duty hours. Ideally, one security guard post could then suffice for two or more buildings.

- Place transient and dependent's service facilities such as exchanges and hospitals near an entrance to minimize traffic flow.

- Segregate commercial (e.g., shipping and receiving) facilities to enhance traffic segregation and control.

- Identify activities that operate on a 24-hour basis and position them to make use of the unpaid surveillance provided.

- Group and position any limited access facilities to minimize the area to be secured.

3.4 Parking Lots

The location and use of parking lots are critical to effective security since items stolen on an installation are traditionally removed by a vehicle. Detailed design of the parking lots may not be completed during installation design, but the security planner should ensure that their locations do not inhibit security measures. Strategies supportive of security are to:

- Use fences or other barriers to channel foot traffic to and from the lots through a few choke-points where observation of the types of material being carried by pedestrians to their cars can be observed.

- Place parking lots near the facility to be supported, but preferably in front of it so access routes can be observed by receptionists or other similar personnel. Parking lots should not be hidden in trees or other areas where surveillance is difficult.

- Provide parking lots for specific types of personnel or patrons of specific facilities.

- Select parking lot locations in conjunction with traffic flow design to minimize unnecessary travel.

4. SUMMARY

The more detailed and well thought out the installation plan, the greater the ultimate level of security will be enhanced, and the lower the costs. Changes at the planning level can be made at little or no cost which will result in substantial savings later. For example, elimination of only one guard post (manned around the clock) can save over $70,000 every year that the installation exists, and reduction in thefts due to the proper location of a parking lot can be equally as

important. The security planner has equally as important a role -- and responsibility -- in making sure such savings are achieved as does any member of the planning team.

CONTINUED

1 OF 3

APPENDIX B

The Large Complex

1. INTRODUCTION

Security engineering for the large complex parallels closely that for an installation. The planner must identify the vulnerabilities of the complex and relate these to the environment in which it exists. The difference is in scale. Where the planner for the *installation* can consider gross traffic flow characteristics, the planner for the *complex* should locate bicycle racks and management parking spaces.

The specific factors to be considered are dependent upon the operational requirements of the complex being planned. The complex used to illustrate the factors to be considered for this discussion is a hospital, since it presents many opportunities for the application of security engineering techniques.

2. SECURITY ENGINEERING CONSIDERATIONS

2.1 Site Plan

Although the location of the complex will normally not be influenced by security considerations, a security planner should be involved in site planning discussions at the earliest possible stages. This introduces both the concept of a security planner and the need to consider security throughout the development cycle. It also familiarizes the security planner with organizational requirements and vulnerabilities. He must work with departmental supervisory personnel to develop safeguards needed for these operations. In the course of these discussions, the security planner will also indoctrinate supervisory personnel with the need to consider security in their planning, and will serve as a moderating influence upon those overreacting to security as well as on those who tend to ignore it.

While the actual location of the site may not be influenced by the security planner, the site plan certainly should be. The proper placement of particular functional areas in a complex is a major factor in achieving a successful security program. In developing the site plan, the security planner should identify the activities to be carried out in each building and should trace the traffic flow required to support each function at various times of the day and night. Vulnerabilities should be assigned, and sensitive items and areas identified. Consideration should be given to closing as many access points as possible during times of decreased activity, and to making the maximum use -- for surveillance -- of activities manned on a 24-hour basis. Other specific engineering considerations are noted below.

2.2 Traffic Control

The traffic control pattern is one of the major elements for consideration in development of the site plan. It includes location of parking areas, direction of traffic flow, and defining access and exit points. The objectives are to: Limit traffic to as few areas as possible so as to minimize opportunities for removal of hospital property; plan parking areas as close as possible to building entry points, while maintaining surveillance; and segregate the types of traffic. If numerous entry points are necessary during the day or operational time period, consideration should be given to the closing of certain of these points during the evening or nonoperational time period. Restricted entry and exit points render it more difficult for a malefactor to escape, and the security force can be more effective as their activity of concentrated surveillance, along with high visibility, can be maximized. Specific attention should be given to how the traffic flow and parking facilities will appear during times of limited operations. For example, nurses working in the early hours of the morning should be provided parking which is under the surveillance of either a guard post, or a station manned 24 hours per day. An example of how parking can be planned to make use of surveillance provided by a security guard post, and to accommodate different types of traffic, is shown in Figure B-1.

2.3 Building Locations

The placement of buildings, parking areas, and building entry and exit points are directly related and require careful correlation. Building locations should provide a clear area between the site perimeter and the building for surveillance. In some cases, the building must be located along the property line and so must provide an element of perimeter protection. In the case of multiple buildings situated close to the property line, a fence or wall connecting the buildings can serve as a good perimeter control, depending on the number and location of building openings. Use of buildings as part of the perimeter security can, however, be detrimental to security and should be avoided if sufficient space is available. If buildings are so used, careful attention must be paid to reducing their vulnerability to intrusion or egress. Walls should be sheer, with no convenient handholds for intruders, and windows should be eliminated or permanently closed.

Building placement is important in avoiding vulnerabilities. For example, in one complex of many buildings, patient care units were scattered throughout the site. A particular problem in this regard was the all-night delivery of emergency drugs from the main pharmacy to these fairly distant buildings. Not only was a vulnerability created for a drug robbery but for an assault as well.

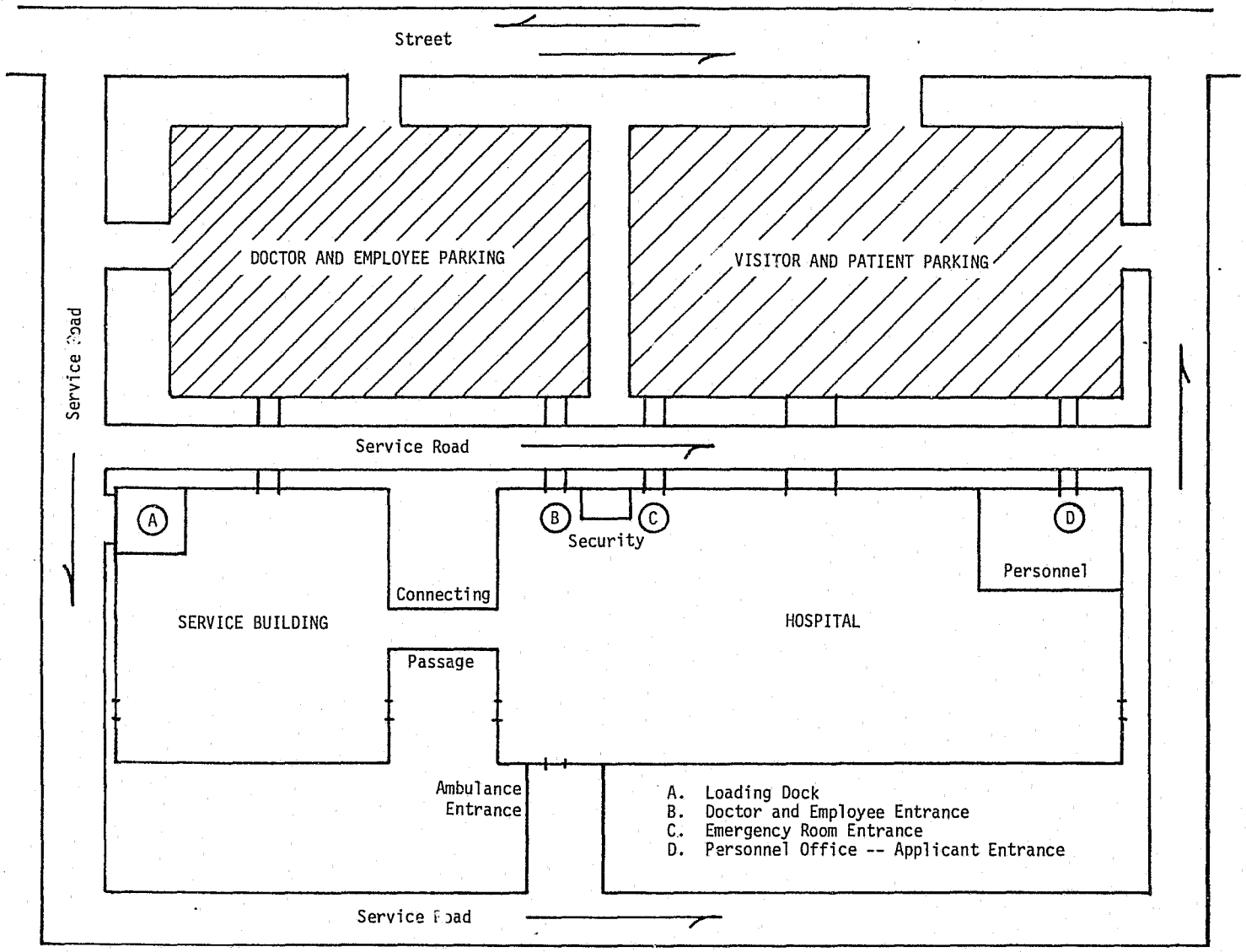


Figure B-1. A Parking and Traffic Pattern Plan

If the security planner had evaluated traffic flow (which includes pedestrians) for the entire 24-hour period, he would have been able to recommend that these facilities be grouped and placed closer to the pharmacy.

During the considerations of building locations, various alternatives should be considered, with maximum use made of opportunities for unpaid surveillance (i.e., if a facility is operational 24 hours per day with patients or workers coming and going, they can serve as unpaid assistants to the security force). In short, every effort should be made to make the physical complex complement the normal operational procedures to produce enhanced security.

3. SECURITY ENGINEERING STRATEGIES

3.1 General

Some of the many strategies to be employed in designing for security are noted below. Their application is a matter of judgment and must be based upon the actual situation, since individual strategies often conflict with one another. For example, delineation of access limits calls for the use of bushes, trees, or mounds, while surveillance would call for a completely open area. Thus, the resulting plan must achieve a compromise. Low bushes, different surfaces, or plantings are used to achieve the maximum security consistent with the situation. Fences have been cited as being counterproductive, but they are often required to clearly define the limits of public egress and for safety. The competent security planner will mix his strategies to achieve his objectives.

3.2 Building Openings

Building openings include not only the normally considered windows and doors but also ventilators, crawl spaces, utility tunnels, interior courtyards, and emergency exits. It has already been established that the fewer the access points, the easier it is to provide surveillance and security. Beyond this basic approach, specific strategies that can be applied are to:

- Designate entrances for employee use only, and limit these as much as possible both as to number and as to hours of operation. While these are operational matters, the locations and types of doors must be determined based upon anticipated use. Location of locker facilities, time clocks, and parking all are affected by the location of such access points.

3.3 Employment and Purchasing Offices

One of the basic premises of security engineering is that decreased exposure results in decreased loss. Therefore, limiting access of facilities to specific categories of personnel only is recommended. Within the complex, positioning offices such as the civilian personnel employment office and the purchasing office away from the main facility is, therefore, advisable. Specific strategies to be employed are to:

- Position the employment office in a separate building with associated parking, if possible. If not, separate it from the facility using a separate entrance and locked doors.
- Separate the purchasing office from the facility, possibly colocating it with the employment office.
- Group functions not requiring access to the hospital complex together, particularly when they attract traffic different from that of the other buildings of the complex.

3.4 Outpatient Areas

The same basic principle applies to outpatient areas as to the employment office. To avoid unnecessary traffic, outpatient areas should not be located deep within the facility. It is often difficult to locate the outpatient area in a separate facility, since common laboratory, x-ray, physical therapy, and pharmacies may support both inpatient and outpatient needs. It is, however, possible to locate the outpatient areas close to an entrance. The location of the outpatient areas must be considered when planning for traffic flow, parking areas, and access points. The security planners must be sensitive to these relationships and point out the implications of decisions made based upon operational requirements.

3.5 Trash Removal

The trash removal facilities provided can also serve as a convenient, and usually ignored, method of removing sizable quantities of hospital property undetected. The location and types of such facilities should be chosen as part of the security plans. Strategies to be used to stop unauthorized use are to:

- Place the containers far enough from the building so individuals using them can be observed.

- Locate receptacles in the view of an office or station manned 24 hours a day.

- Illuminate the area.

If outside laundry services are used, similar care should be provided in the heavy-traffic areas.

3.6 Lighting

Good lighting is an inexpensive method for increasing security. For best results, the area lighted should be under surveillance, but lighting will serve as a deterrent even if no active surveillance is maintained. Psychological studies show that individuals perpetrating crime in the hours of darkness have a psychological fear of light itself. Lighting always should be considered during the development of the complex plan especially in relation to parking access points and pedestrian corridors. Some specific strategies are to:

- Position lighting to enhance surveillance of parking areas, particularly those positions to be used late at night.

- Provide lighting of pedestrian corridors from parking areas to access points.

- Light areas where losses could occur, or which could provide convenient places to transfer stolen items (i.e., trash receptacles, any unlocked doors not under surveillance).

- Light authorized access points.

The following guides should be observed when designing lighting installations to minimize vandalism and maintain illumination levels:

- Use break resistant lenses.

- Illuminate parking lots, using 14-foot-minimum-height light poles.

- Illuminate buildings with fixtures mounted on 14-foot-minimum-height light poles.
- Have lighting directed at the facility when building is to be patrolled from exterior.
- Have lighting directed to illuminate grounds around the facility when building is to be patrolled from within.
- Use increased levels of illumination at potential points of access into buildings.
- Illuminate walkways with 14-foot-minimum-height lights.

3.7 Shipping and Receiving

The routing and handling of commercial traffic always deserves specific consideration. In a hospital, the items being received are often of high value and small bulk, as well as sensitive in nature (i.e., drugs). Shipped items are usually not so valuable nor as numerous. Therefore, separation of shipping and receiving points may not be practical. However, separation should be considered, for the colocation of these functions provides an ideal situation for pilferage and large-scale theft. Strategies applicable are to:

- Provide as short an access and egress route as possible.
- Separate commercial traffic from user and employee traffic.
- Position docks so shipments are separate from receiving points.
- Provide high intensity of illumination to ensure visibility.
- Locate shipping and receiving facilities where they are overlooked by offices occupied by management personnel.

4. SUMMARY

Integration of the various elements that must be considered in the development of the plan for a complex is a difficult undertaking. However, its accomplishment will pay dividends in lower costs for security and decreased losses for the life of the complex.

APPENDIX C

The Individual Building

1. INTRODUCTION

Security engineering for the individual building should consider the perimeter to control unauthorized entry, access points to channel and segregate types of traffic, interior design to enhance surveillance, and location of sensitive items or operations to maximize passive protection. As in other areas, security planning should be initiated as early in the design stage as possible, and provisions for security-related wiring and hardware should be incorporated at the initial stages.

The application of security engineering concepts, strategies, and standards will vary somewhat with individual building requirements, but the basics, discussed below, remain the same.

2. SECURITY ENGINEERING CONSIDERATIONS

2.1 Building Design

Architectural sketches and diagrams of any building should be closely examined by the security planner. Many examples exist where buildings are so designed that a series of steps are provided to the roof by an ornamental facade, or where multiple access points are provided by ground height windows shielded from observation by plantings. Objections to such features at the design stage will usually be effective where they may not be at a later stage of construction. Such deterrents to good security are readily identifiable -- *if designs are examined for that purpose.* Unless that responsibility is assigned, however, it may never be accomplished, and an obvious security hazard will be created during construction.

In addition to such exterior design features, the interior groupings of facilities, and locations of corridors, elevators, offices, and sensitive item storage or operations must be examined. As a rule of thumb, the more visibility the better, and the creation of blind spots or areas not subject to routine surveillance should be avoided.

Proper design can also have a positive influence upon the ways a building is used. Proper use can be encouraged by providing appropriate facilities that: (a) By their general nature, will not attract antisocial user groups; (b) by their design, will preclude antisocial groups; and (c) incorporate counteroffensive elements or mechanisms to reduce criminal opportunities and/or improve response time of security personnel following an incident. These facilities might include areas such as: Public restrooms, vending areas, equipment areas, and routes of access or egress (i.e., elevators, garages, and corridors). These areas should be designed in ways that prevent or discourage use for counterproductive or dangerous purposes. Design considerations might include locating the facilities where they can be more easily monitored, sizing the facilities for optimum control and to discourage use for purposes

other than those intended, and providing control devices to restrict use to only authorized persons (e.g., closed-circuit television cameras, communications equipment, alarm systems, and lighting fixtures that can be used to increase the surveillability of the facilities and improve response time of security personnel). Also, the security engineering considerations and strategies for a large complex apply to the individual building and its exterior and perimeter. Grounds should be free of rocks and other debris; trees and shrubs should not obscure observation; and bushes or shrubs should be used to channel pedestrian flow.

2.2 Access Control

Access to a building should be designed to facilitate surveillance, control, and segregation of traffic by function. Dependent upon the functions to be accomplished by the occupants, access points should be designated as either to be closed during nonduty hours, or to be subject to surveillance and control for all-hours entry. Alarms should be installed at closed access and exit points to alert a guard to their unauthorized use. When building guards are to be employed, guard stations should be so designed and located that one station can observe and control as many access points as possible.

2.3 Surveillance

With the ever increasing costs of manpower, maximum use must be made of the security provided by the normal occupants of the building. In many cases, this can best be accomplished by proper scheduling of activities such as by arranging for cleaning or maintenance personnel to be present during nonduty hours. The presence of such personnel in a facility during the hours when it is normally unoccupied serves as a deterrent to unauthorized entry. The security planner can also do his part by ensuring that the design and locations of offices, corridors, elevators, access points, and manned stations facilitate observation by and of their users. A secretary station permitting a view of the corridor outside through a glass partition enhances observation -- and identification -- of unauthorized visitors. Receptionist desks permitting a view of access points and elevator banks add an additional (unpaid) guard post during duty hours.

2.4 Sensitive Items or Operations

Where the use to which the building will be put is known, sensitive item storage or operations can be identified. Examples of sensitive item storage are drugs in a hospital complex, precious metals in an industrial operation, classified material in a military operation, or a computer or communications complex where access must be controlled. The facilities for these should be located to minimize traffic by unauthorized personnel and to provide maximum deterrence to covert access and egress. Location on a perimeter wall should be avoided. Natural surveillance should be enhanced by the location of access points wherever possible.

3. SECURITY ENGINEERING STRATEGIES

It is stating the obvious to point out that the greatest majority of thefts take place within a building and that most are crimes of opportunity committed by individuals authorized access to the facility. In spite of this, however, most security planning concentrates on keeping out unauthorized intruders. Security engineering strategies (and standards) include design to restrict unauthorized entry, and the security planner must certainly observe them. He should also, however, be fully cognizant of how the spatial relationship of the building interior can be planned to decrease the exposure of pilferable items or to increase the risk of detection. Nearly all of the concepts and strategies presented throughout this report are applicable, depending upon the type building being considered. Noted below are strategies having general applicability.

3.1 Building Openings

Building openings include doors, windows, skylights, crawl spaces, utility tunnels, emergency exits, and any other route of access not through a wall. It is obvious that the fewer the openings, the easier the task of surveillance and control. Strategies that can be used to increase security are to:

- Locate windows on the ground floor as high as possible above ground level, and design them to restrict entry.
- Place bars on the inside of windows or other openings where breaking the window will activate an alarm.
- Wire emergency exits and those to be closed during portions of the day so alarms will be activated if used.
- Position receptionist desks or guard posts so that access points, including elevators, are under surveillance.
- Design access points so that routes to and from them are under surveillance, preferably by management representatives.

3.2 Elevators

Entry and exit routes to a building should be so designed that they can be monitored. This is particularly true of elevator banks servicing a garage or commercial area as well as an office or industrial complex. Strategies which can be employed are to:

- Program elevators so that separate elevators service the different sections of the building, requiring transfers at the ground floor within sight of a guard or receptionist.

- Design separate elevator banks with one servicing the garage or lower levels, the other the office complex.

3.3 Surveillance

One of the best deterrents to crime is the knowledge that your act can be observed. Therefore, every effort should be made to incorporate design features permitting surveillance. Some effective strategies are to:

- Use open spaces whenever possible and avoid any design creating blind spots where criminal acts could be committed undetected.

- Eliminate columns and partitions that restrict vision.

- Use open space or glass partitions, doors, and windows around work stations to permit surveillance.

- Incorporate wiring for surveillance devices, such as closed-circuit TV, in building plans.

- Position any continuously manned operations so that their occupants will provide natural surveillance of critical areas.

3.4 Construction Considerations

In addition to the more generally applicable strategies noted, there are a number of security strategies that are applicable to building design. Some of these which should be observed or avoided are listed below.

Exterior Walls and Roofs

- The following are conducive to security:

  - Walls designed to prevent roof access.

  - Flush, wall-mounted fixtures to deny handholds for climbing.

- Walls with a minimum of 12-foot height.

- The following should be avoided:

  - Decorative wall finish patterns and recesses for lighting fixtures that are climbable.

  - Half-walls or free-standing walls connected to buildings.

  - Recesses that provide concealment (e.g., recessed entrances, patios, accessible courtyards).

  - Low, covered walkways.

  - False wall fronts and/or wide roof overhangs.

Windows, Skylights, and Transoms

- The following are conducive to security:

  - Eliminate exterior window sills.

  - Eliminate ground-floor windows.

  - Use minimum number of windows.

  - Use ceiling-level, horizontal strip windows (8-inch width maximum).

  - Install window frames to place putty on the interior.

- The following should be avoided:

  - Skylights.

  - Transoms on exterior door.

  - Breakable glass in windows.

  - Windows within 8 feet of ground level and 4 feet of doors.

Doors (Frames, Hardware, Locks and Keys, Openings)

- The following are conducive to security:
  - Minimum number of exterior doorways.
  - Locks for elevator doors.
  - One-inch minimum bolt length for all throw bolts used.
  - Ceiling-to-floor zone gates for selected building usage after hours.
  - Astragals on all double doors with panic hardware.
  - Inside located, and lockable throw bolts for roof hatches.
  - Nonremovable pins in door hinges.
  - Key-operated locks with removable cores which can be changed after construction is complete if desired.
  - Elimination of master-keyed locks, if and when possible, and strict control of a minimum number of master keys where it is not.
  - Keys that require factory duplication.
  - Exterior handle and lock access at main entrance only.
  - Lockable slide bolts for overhead doors in addition to cylinder or padlock.
  - Provision for securing operating shaft on crank-operated door as well as cylinder or padlock.
  - Pry-proof metal door frames.
- The following should be avoided:
  - Surface-mounted locks.
  - Locks having knob-mounted key access.

- Exterior doorways for restrooms that also open into interior of building.

- Doors to building exterior in secured storage areas.

- Recessed interior doorways.

- Doors on restrooms (use a maze instead).

- Windows in exterior doors.

- Sliding doors.

3.5 Additional Strategies

The following groups of design strategies are all important when considering the overall building design, with the primary intent being the reduction of destruction of property. A number of these also contribute to the concepts of access control and surveillance -- the primary means of inhibiting criminal offenders.

- Heating, air-conditioning, and ventilation units recessed in walls with locked covers flush with wall.

- Baffles for grills covering utility tunnels and vents.

- Strong grills on all utility tunnel openings, vents, and manholes.

- Key-controlled light fixtures in all public areas, with standard light controls for offices.

- Secured roof fans.

- Switches for exterior lighting located in secured areas, not hallways.

- Automatic controls for night lighting of corridors.

- Interior walls and ceilings:

  - Epoxy-coated, or equal, concrete or concrete block walls in restrooms.

- Hard-glazed wainscoting on all walls.

- Epoxy coating, or equal, throughout corridors.

- Ceramic tile or block wainscoting on all corridor walls.

- Restrooms:

  - Heavy-duty fixtures.

  - Fireproof trash disposal containers.

  - Floor- and ceiling-mounted stall partitions.

  - Recessed shelves.

  - Burn- or scorch-proof commode seats.

  - Fewer restrooms with larger capacities each.

  - Hand-washing facilities located in hall alcoves, with minimal closed areas for commodes and/or urinals.

- Vaults and storage areas:

  - Solid reinforced walls to true ceiling height in all secured storage areas and vaults.

  - Mechanical ventilation and no windows for secured storage areas.

  - Secured storage areas located throughout buildings to provide safe storage for high-value equipment.

- Hallways, stairwells, and elevators;

  - Straight hallways.

  - No large enclosed stairwells.

  - Heavy-duty railings for stairwells.

- Stainless steel elevator control buttons.
- Elimination of all possible corridors.
- Kickplate to the floor on stair risers.

- Mechanical and custodial rooms:
  - Machinery controls located in a single secured area with a locked control panel.
  - Custodial room large enough to provide secured storage for ladders.
  - Special paint locker secured against entry and located well away from main building.

4. SUMMARY

The most important aspect in applying security engineering principles to any facility is to ensure their consideration at the planning stage.

Even if a strategy is not considered necessary for the initial uses forecast, but might be required later, it would be cost-effective to include as much of the strategy as possible (e.g., wiring for an alarm system without actually installing the equipment) rather than to have to renovate in the future.

APPENDIX D

Renovation

1. INTRODUCTION

Security engineering concepts and strategies applicable to the planning, design, and construction stages of a facility are also applicable to renovation of existing facilities. However, there are limitations on the concepts that are applicable at the renovation stage. Each change desired must be assessed in terms of practicality and cost effectiveness. For example, moving an entrance to improve access control might be advisable or might be neither practical nor cost-effective. The security planner is always constrained by cost considerations, and the least costly changes will be best received. On the positive side, loss data may be available, and the security planner is dealing with established procedures and a defined security plan. Therefore, he can design his strategies to counter known security problems.

Basic principles remain the same. The security planner should become involved in the renovation process as early as possible. He should become thoroughly familiar with the operational objectives desired and should, whenever practical, concentrate upon changes requiring relocations and refurbishing, rather than complete change. Although the security planner is somewhat constrained since he must accommodate his plan to an existing facility, it is in remodeling or renovation of facilities that he will most often have a chance to enhance security. Therefore, security planners should take advantage of such occasions to upgrade protection and to progress towards their ultimate goals.

2. SECURITY MASTER PLAN

Every security planner responsible for a building, a complex, or an installation should have a master plan that details the improvements he desires to enhance security. (The bases for such plans and suggested considerations are contained in Appendices A through C, and in the body of this report.) With such a plan, every renovation project will provide an opportunity for implementing a portion of the plan. For example, alarm wiring can be included in new construction, newly added or modified doors can be positioned and constructed to improve security, new parking lots can have access and exit points redesigned, and lighting can be improved. Once a portion of the plan is implemented, securing the next portion is made easier. Examples of strategies for improvement that can be made at minimal cost, which are particularly applicable during renovation or remodeling, are

presented in Section 3 of this appendix. The plan should also identify existing features and structures whose demolition and removal could enhance facility security.

3. RENOVATION STRATEGIES

3.1 General

Security engineering strategies easily accomplished during renovation or remodeling of existing facilities are noted below. They are drawn from actual strategies being implemented at CPTED demonstration sites.

3.2 Landscaping

Access control and surveillance can be enhanced by the proper use of landscaping techniques. Some applicable strategies are to:

- Use low bushes to delineate access routes, and public, semipublic, and private areas.
- Install additional lighting around parking lots, entrances, and secluded areas.
- Use mounds or ditches to restrict vehicular travel.

3.3 Parking

Parking areas are normally provided for vehicles and bicycles. The security strategies applicable to both are similar. Some strategies to be applied are to:

- Place areas where the owners can observe them during their work periods.
- Restrict entry to any through vehicles by using deadends and restricted entry points.
- Restrict entry and exit points for pedestrians going to or from their vehicles to routes or points under surveillance.

3.4 Painting

Murals, graphic designs, and even different-colored paint can be used to distinguish between areas used for different purposes. If individuals can distinguish those who are authorized in the area from those who are not, natural surveillance can be enhanced. Some strategies are to:

- Paint colored strips or walls to serve as guides between, or to differentiate, services or functions.
- Develop and paint graphic wall designs to designate the functions being performed in the area.

3.5 Surveillance

Increased surveillance can be achieved during renovation through the judicious use of materials, redesign of corridors or stairwells, and repositioning of desks. Strategies that can be applied are to:

- Station secretaries' desks to face corridors, and use glass windows, glass doors, or open spaces to facilitate surveillance.
- Block off unused or dead space that cannot be readily observed (e.g., under stairwells, crawl spaces).
- Eliminate bends or jogs in corridors.
- Move stations manned 24 hours to permit better surveillance of the facility, particularly storage areas where sensitive items are kept.

3.6 Hardware

Security engineering requires the use of burglar-resistant hardware. The renovation stage provides an excellent opportunity to ensure that good security standards are met. Dependent upon the extent of renovation, the opportunity to install surveillance gear is also provided. Some specific areas to consider are:

- Doors with hinges on the secured side, jimmy- and pick-resistant locks and door/door jam materials.

- Adequate wiring to support good interior and exterior lighting.

- Burglar- and vandal-resistant glass.

- Buried conduit of adequate capacity to route the cabling of proprietary television and alarm monitoring and control systems.

4. SUMMARY

Security measures should be considered in any renovation. The best results will be obtained if the security planner has a master plan to guide his efforts. Incorporation of wiring for security alarms, glass partitions for increased surveillance, or upgrading of locks and doors can be accomplished at little increased cost as part of another project although not justifiable by themselves. Security engineering concepts and strategies applicable to facilities construction are equally applicable to renovation.

APPENDIX E

Sources of Consultant Services in Environmental/Industrial Security

This appendix presents a list of firms, companies, and/or individuals who provide consultant services in the area of environmental/industrial security. It is not suggested that all possible sources were exhausted prior to compilation of this list; however, every effort has been made to provide a completely respresentative cross section of expertise.

Because the range of services provided by these firms varies widely -- some are highly specialized (e.g., design and fabrication of devices) and some direct their attention to a broad range of security problems (e.g., human factors, management, hardware) -- this list has been presented alphabetically and coded into four categories that are pertinent to the solution of security problems in Navy-operated facilities and industrial complexes. Each entry contains the firm's name, address, telephone number, a brief description of the services that firm provides, and category code letters (i.e., P=planning; D=design; C=construction, including hardware design, fabrication and installation; G=general). Many of the firms are coded to more than one category.

Airport Security Council
97-45 Queens Boulevard
Forest Hills, New York 11374

Phone: (212) 275-9300

The Council, which is responsible for developing and administering air cargo loss prevention programs for LaGuardia, Kennedy, and Newark Airports, provides consultants on airport security and security of air cargo. Areas of primary concern are: Personnel security, physical facilities inspection, operational security programs, analysis and evaluation of loss data, and liaison with law enforcement agencies.

(P/D)

Alarm Security Konsultants
Division of Security Architects, Inc.
P.O. Box 182
Medford, New Jersey 90955

Phone: (609) 654-5333

This company provides analysis and assessment of security problems for residential, institutional, educational, industrial, and commercial applications.

(P)

The American Institute of Architects
Committee on Architure for Justice
1735 New York Avenue, NW
Washington, DC 20006

Phone: (202) 785-7300

This Committee is comprised of architects who are primarily concerned with the planning and design of police and correctional facilities. However, since the members are, by necessity, knowledgeable in the areas of architectural design that impact on criminal justice and crime prevention, they are capable of applying those concepts to virtually any environment. The members of AIA's Committee on Architecture for Justice are as follows:

(P/D)

Raymond C. Abst, AIA
ABST-GROTHE & ASSOC.
624 Scenic Dr.
Modesto, California 95350
209/529-2682

Gerald Deines, AID
Gerald Deines & Assoc. Arch.
136 S. Wolcott
Casper, Wyoming 82601
307/266-2616

Alton L. Akins, AIA
Texas Department of Corrections
Box 99
Huntsville, Texas 77340
713/295-6371

Leroy Andrews, AIA
344 Lynnbrook Avenue
Ventura, California 93003

Joe Boehning, AIA
Boehning, Protz, & Assoc.
2005 Carlisle Boulevard, NE
Albuquerque, New Mexico 87110
505/268-8785

Daniel Boone, Jr. AIA
Boone & Pope, Inc.
224 S. Leggett Drive
Abilene, Texas 79605
915/673-7334

Pamela J. Clayton, AIA
Space for Social Systems
100 S. Patrick St.
Alexandria, Virginia 22314
703/683-1957

Leon Clemmer, AIA
Leon Clemmer & Associates
445 Cedar Street
Jenkintown, Pennsylvania 13046
215/885-6666

Richard G. Conklin, AIA
DMJM
3250 Wilshire Boulevard
Los Angeles, California 90010
213/381-3663

William T. Davis, AIA
12 Washington Park, East
Washington St.
Greenville, South Carolina 29601
803/242-0761

William L. Ensign, FAIA
McLeod, Ferrara & Ensign
5454 Wisconsin Ave. NW
Washington, D.C. 20015
202/652-2775

Sidney J. Folse, Jr., AIA
Folse/HDR
1440 Canal St., Suite 2120
New Orleans, Louisiana 70112
504/525-1444

Robert O. Geary, AIA
Geary, Moore & Aherens, Inc.
1720 Euclid Avenue
Cleveland, Ohio 44115
216/621-7770

Albert Gilbert
Ballinger
841 Chestnut St.
Philadelphia, Pennsylvania 19107
215/629-0900

Thomas E. Greacen, II, FAIA
Greacen, Houston & Rogers
3220 Louisiana, Suite 205
Houston, Texas 77006
713/529-4644

Walter F. Greene, Jr., AIA
Associated Architects
Spring Lane
Farmington, Connecticut 06032
203/677-2801

Robert B. Groenleer
Michigan State Dept. of Corrections
PO Box 30003, Logan Center
Lansing, Michigan 48909
517/373-2461

David B. Hall, AIA
Ellerbe Architects
1 Appletree Square
Bloomington, Minnesota 55420
612/853-2277

Ira Kessler, AIA
The Ofc. of Ira Kessler
980 Benton St.
Woodmere, New York 11598
516/374-1900

George F. Klein, Jr., AIA
Parker, Klein Associates
430 Oak Grove
Minneapolis, Minnesota 55403
612/871-6864

Joseph N. Ladd, AIA
Marcellus Wright Cox & Ladd
1501 N. Hamilton St.
Richmond, Virginia 23230
804/358-7181

Tony R. Lang, AIA
Phillips Swager Assoc., Inc.
3622 Knoxville Avenue
Peoria, Illinois 61603
309/688-9511

Victor D. Langhart, AIA
RNL/Interplan
1610 Arapahoe Street, A-300
Denver, Colorado 80202
303/573-1331

C. Theodore Larson, FAIA
Univ. of Michigan
3575 E. Huron River Drive
Ann Arbor, Michigan 48104
313/971-6274

Patrick Leamy, AIA
HOK
915 Front Street
San Francisco, Calif. 94111
415/271-4848 or 415/986-4275

Jimmy Dan Maddox, AIA
Little-Maddox-Standefer
402 S. Main Street PO 6
Jonesboro, Arkansas 72401

E. Frank McLane, Jr., AIA
100 N. Ashley #800
Tampa, Florida 33602

Robert F. Messmer, AIA
Bureau of Prisons/US Dept. of Justice
320 First Street, NW
Washington, D.C. 20534
202/724-3249

Walter H. Moleski, AIA
Environmental Research Group
1821 Sansom Street
Philadelphia, Pennsylvania 19103

John C. Monroe, Jr., AIA
Monroe & Lefebvre
1021 Pennsylvania
Kansas City, Missouri 64105
816/421-7478

Frederic D. Moyer, AIA
NCCJPA
505 E. Green Street #200
Champaign, Illinois 61820
217/333-0312

Fred G. Owles, Jr., AIA
1819 W. Colonial Drive
Orlando, Florida 32804

Lester C. Pancoast, AIA
Pancoast, Barrelli, Albaisa, Archts.
3370 Mary Street
Miami, Florida 33133
305/442-1193

Caraker D. Paschal, AIA
Finch, Alexander, Barnes, Rothschild & Paschal
44 Broad Street, NW
Atlanta, Georgia 30303
404/688-3313

John McGough, FAIA
Walker. McGough, Foltz, Lyerla
North 120 Wall Street
Spokane, Washington 99201
509/838-8681

Gordon C. Pierce, AIA
219 S. Pennsylvania Avenue
Greensburg, Pennsylvania 15601
412/834-3890

Fred Powers
HOK
100 N. Broadway St.
St. Louis, Missouri 63102
314/421-2000

Ted H. Prindle, AIA
Prindle & Patrick
301 Pierce Street
Clearwater, Florida 33516

Bruce C. Reams, AIA
Orput Associates
1607 North Alpine Road
Rockford, Illinois 61107
815/398-8785

Kenneth Ricci, AIA
The Ehrenkrantz Group, P.C.
19 W. 44th Street
New York, New York 10036
212/889-0099

Harold D. Robertson, AIA
Leo A. Daly Company
8600 Indian Hills Drive
Omaha, Nebraska 68114
402/391-8111

Elliott P. Rothman, AIA
156 Milk Street
Boston, Massachusetts 02109
617/482-5140

Allen L. Patrick, AIA
Prindle & Patrick
199 South Fifth Street
Columbus, Ohio 43215
614/228-3233

Paul Silver, AIA
Gruzen & Partners
1700 Broadway
New York, New York 10019
212/582-7090

Walter H. Sobel, FAIA
Walter H. Sobel, FAIA & Associates
2 North Riverside Plaza
Chicago, Illinois 60606
312/263-6324

George W. Sprinkle, FAIA
Guirey/Srnka/Arnold & Sprinkle
3122 N. Third Avenue
Phoenix, Arizona 85013
602/264-0217

J. Oliver Stein, AIA
Hayes, Seay, Mattern & Mattern
1315 Franklin Road, SW
PO Box 13446
Roanoke, Virginia 24016
703/343-6971

G. John Stevens, AIA
John Stevens Assocs. Inc.
511 East Larned St.
Detroit, Michigan 48226
313/964-0700

Earl S. Swensson, AIA
Earl Swensson Associates
2303 21st Avenue, S., 4th Fl.
Nashville, Tennessee 37212
615/388-2782

William H. Switzer, AIA
Wm. H. Switzer & Assoc.
984 N. Broadway
Yonkers, New York 10701
914/423-5500

Martha L. Rothman, AIA
156 Milk Street
Boston, Massachusetts 02109
617/482-5140

Thomas B. Tucker, AIA
Tucker, Sadler & Associates
2411 Second Avenue
San Diego, California 92101
714/236-1662

Ronald Richard Rucinski, AIA
Donald J. Stephens Assoc. Arch.
41 State Street
Albany, New York 12207
518/462-6551

DeNorval Unthank, Jr. AIA
Unthank Seder & Poticha Architects
259 East Fifth Avenue
Eugene, Oregon 97401
503/342-5777

William H. Vanderbout, AIA
WRDC Architects, Planners, Engineers
150 Ann St. NW
Grand Rapids, Michigan 49502
616/363-9007

Ronald E. Vaughn, AIA
Goat Hill Rd.
PO Box 265
Lambertville, New Jersey 08530
609/397-0801

R. W. Wening, Jr., AIA
Mills, Clagett & Wening
1720 Eye Street N.W.
Washington, DC 20006
202/833-8940

Herbert Wettstein, AIA
N.J. State Div. of Bldg. & Constr.
P.O. Box 1243
Trenton, New Jersey 08625
609/292-5018

W. Gene Williams, AIA
W. Gene Williams & Assocs.
3150 Liberty Tower
Oklahoma City, Oklahoma 73102
405/232-6521

Norman E. Wirkler, AIA
DDDKG Architects
1122 Rockdale Road
Dubuque, Iowa 52001
319/583-9131

R. Lamar Youngblood, AIA
Barnes, Landes, Goodman, Youngblood
1000W. 38th Street, #100
Austin, Texas 78731
512/451-8281

David Miles Ziskind, AIA
Curtis & Davis
126 E. 38th Street
New York, New York 10016
212/689-9590

Anacapa Sciences, Incorporated
P.O. Drawer Q
2034 De La Vina
Santa Barbara, California 93102

Phone: (805) 966-6157

This company provides research, training, and consulting services in the behavioral and engineering sciences. Interest in law enforcement involves: Evaluation of systems, equipment, and procedures from the user viewpoint, evaluation of crime reduction programs, development of law-enforcement techniques and methods, the conduct of pertinent training programs and law enforcement information processing systems. Classes and research emphasize: White-collar crime, urban terrorism, burglary, intelligence analysis, and management and tactical decisionmaking. Services are rendered to government agencies, industries, and commercial concerns.

(G)

Analytical Systems Engineering Corporation
25 Ray Avenue
Burlington, Massachusetts 01803

Phone: (617) 272-7910

This company has experience in law enforcement, criminal justice consulting, and security systems, including the specific areas of sensor applications, human factors considerations, and data base management. The company specializes in objective studies and analyses designed to solve a user's specific problems. For example, systems have been devised to prevent pilferage of inventory and physical plant items as well as the loss of proprietary data and secrets through the activities of business intelligence and espionage operatives.

(G)

Andres Inn Research Center
School of Law, Southern Methodist University
Dallas, Texas 75275

Phone: (214) 692-3380

This organization offers a research capability for police and industrial security forces. Evaluation programs are offered, involving both the selection of a system and the design of evaluation instruments such as rating scales. Implementation and research is combined in the information retrieval systems areas. Associates are experienced in areas such as accounting, law, operations research, and building flow pattern design.

(P/D)

Anticipation, Inc.
410 Jericho Turnpike
Jericho, New York 11753

Phone: (516) 922-8338

This company provides consultation services specializing in internal theft, including the design of closed-circuit television monitoring equipment, pilferage control devices, and cargo security systems.

(C)

Barnes Engineering Company
30 Commerce Road
Stamford, Connecticut 06904

Phone: (203) 348-5381

This company designs and fabricates sophisticated security devices that meet unique government and industrial specifications. Previous customers include the Atomic Energy Commission and the U.S. Army. The firm has government clearances for highly classified work.

(C)

Bellaire Associates
331 Madison Avenue
New York, New York 10017

Phone: (212) 682-2128

This firm, comprised of professional engineers, specializes in management consulting and performs security surveys. In addition, associates conduct security seminars on such topics as the security of high-rise buildings.

(G)

Benedict & Myrick, Inc.
Office of Special Services
4332 Rhoda Drive
Baton Rouge, Louisiana 70816

Phone: (504) 293-4260 (Baton Rouge)
(504) 581-4222 (New Orleans)

This company provides security consultation, installs equipment for specific security needs, and custom designs and manufactures security items and systems. Surveillance equipment, closed-circuit television, parking access control, and communications systems are used for deterrence, detection, and control. The company develops security planning for new operations, assists in policy planning and prepares manuals of security procedures and personnel training for "turnkey" programs. Previous experience includes U.S. Army intelligence and security.

(C)

CES Telecommunications
511 Golf Mill
Niles, Illinois 60648

Phone: (312) 297-2366

This company offers architectural and engineering support services for the design of security systems for new buildings or for the remodeling of older structures. Services include the survey of facilities in order to determine security problems.

(P/D)

Don D. Darling & Associates
1100 Glendon Avenue
Westwood Center - Suite 901
Los Angeles, California 90024

Phone: (213) 473-6544

This firm, staffed by scientists, engineers, and security specialists, provides consulting services in such areas as: Planning and analyses of security programs and systems, evaluation and testing of existing systems and programs, security systems support, and evaluation and testing of security systems and equipment. Previous consultation has been provided to a cross section of business, industry, institution, and government/military agencies. The firm's collective problemsolving capabilities have led to the establishment of many security standards.

(P/C)

D-CO-Inc.
P.O. Box 5362
Santa Fe, New Mexico 87501

Phone: (505) 983-1594

This company provides consulting, planning and assessment services for high-level security applications. Capabilities include: Electronic engineering, engineering analysis, planning and layout, cost estimates, and report documentation. Security equipment recommendations are made on the basis of product performance and reliability; essential items can be fabricated when proper off-the-shelf components are not available. Clients have included the U.S. Army and National Guard.

(P/D/C)

Tom Finley & Associates
1511 K Street, N.W., Suite 410
Washington, D.C. 20005

Phone: (202) 293-4327

This firm provides consulting services on the problems of cargo theft and pilferage for industrial and government installations. Services include the development of methods for approaching the problem, hardware recommendations, monitoring of installations, and the training of employees on new security equipment.

(G)

Gage-Babcock & Associates Inc.
9836 W. Roosevelt Road
P.O. Box 270
Westchester, Illinois 60153

Phone: (312) 345-8541

This firm specializes in integrating fire protection, safety, and security into systems design. Criteria for the security of buildings and premises are developed for architects. Problems such as personnel, equipment, and physical structure are examined in risk analyses of present buildings.

(P/D)

Harris & Walsh Management Consultants, Inc.
P.O. Box 698 (271 North Avenue)
New Rochelle, New York 10802

Phone: (914) 576-0820

This firm offers comprehensive consulting services on security vulnerability studies, including risk appraisals, dollar loss,

critical loss ratios; countermeasures selection and design, compromising alarms, fences, lights, and other electronic devices; and crime prevention through proper staffing and training of security personnel. Plant protection, fire and disaster control, emergency preparedness, fraud and theft prevention, and the overall protection of physical and informational assets are also areas of capability.

(G)

Richard J. Healy
Building C101, Mail Station 592
The Aerospace Corporation
P.O. Box 92957
Los Angeles, California 90009

Phone: (213) 648-5362

An independent consultant providing services to define the expected hazards to security, and design a defense that applies modern methods and equipment to raise the security level and reduce protection costs. All aspects of potential designs are covered, from plant layout to locks to alarms and lighting.

(G)

Lewis H. Irving, Consultant
Department of Sociology
Central State University
Edmond, Oklahoma 73034

Phone: (405) 341-2980 x2533

An independent consultant who provides social survey research to government agencies and businesses, specializing in defining the human factors approach, both in defining the environment necessary to produce social change and social integration, and in identifying types and kinds of equipment needed to work on the problem.

(P)

Management Safeguards, Inc.
National Headquarters, Two Park Avenue
New York, New York 10016

Phone: (212) 532-7150

The Consulting Division of Management Safeguards offers surveys of physical security, operational procedures, and accounting controls to identify exposures to loss, and to enable development and implementation of security plans. Physical security planning defines the need for alarm and locking devices, employee and visitor controls, communications, lighting, access controls, shipping and receiving dock protection, annunciator consoles, manpower deployment, and security requirements in new buildings or existing facilities.

(G)

Malborough Intelligence
P. O. Box 13
Upper Marlboro, Maryland 20870

Phone: (301) 952-0909

This firm offers a variety of services, including security consulting. Procedures consist of investigation of activities such as internal theft, embezzlement, and pilferage; consulting services are available for the design of internal controls for personnel, equipment, and premises. Recommendations for security systems are made for business and industry after surveys of premises and operations.

(G)

McManis Associates, Inc.
1120 Connecticut Avenue, N.W.
Washington, D. C. 20036

Phone: (202) 296-1355

This firm employs systems engineering methodology to develop pre-architectural specifications for operational configurations including security. Attention is given to security program planning and evaluation, defining objectives, identifying protective needs, and allocating resources.

(P)

George P. Morse & Associates
Consultants in Protection
9402 Stateside Court
Silver Spring, Maryland 20903

Phone: (301) 434-3245

This firm performs studies, provides training, and recommends operational and physical improvements in the area of crime and loss prevention. Specializing in institutional security, particularly hospitals, they perform objective studies and recommend specific solutions. Security systems design and installation support can also be provided.

(P/D)

Mt. San Antonio College
Department of Public Safety and Service
110 North Grand Avenue
Walnut, California 91789

Phone: (213) 339-7331
(714) 595-2211 x252, x324

This organization provides staff personnel who analyze and interpret research data, which are then applied to the design and development of security-related programs.

(P/D)

Robert James Obenland
P. O. Box 139
Concord, New Hampshire 03301

Phone: (603) 284-6407

An independent consultant who provides services in research, programming, architectural design, and postoccupancy evaluation for the built environment. Previous experience has included areas such as architectural and environmental security analyses for courts and correctional facilities, and design assistance focusing on crime prevention and humanization in public housing.

(P/D)

James W. O'Neil, Inc.
25 Massachusetts Avenue
Braintree, Massachusetts 02184

Phone: (617) 843-8653

An independent consultant specializing in preventing losses from burglary, employee theft, robbery, vandalism, espionage, and other criminal activities. Consultation is available for help with problem assessment, analysis of procedures and techniques, improvement in security equipment and service, supervision of acquisition and installation of systems and devices and review of overall security conditions. Surveys include the evaluation of physical security arrangements, review of personnel hiring and training in security, comparison of security policies versus actual practices, and recommendations for developing and implementing security programs.

(G)

PRC Public Management Services, Inc. (PRC/PMS)
7600 Old Springhouse Road
McLean, Virginia 22101

Phone: (703) 893-1830

This company provides services to public and private agencies for organizational and management analysis, program evaluation, resource allocation, information systems design and implementation, facilities design, crime-specific planning, evaluation of anticrime countermeasures, design of correctional systems, and the training of personnel for administration, fiscal control and reporting.

(P/D)

Pacemaker Planning
3617 Lexington Road
Louisville, Kentucky 40207

Phone: (502) 897-5756
(502) 454-0225

This firm analyzes, evaluates, and makes recommendations on how to reduce the loss of cash and high-value merchandise due to employee theft, shoplifting, armed robbery, and burglary. Crime reduction recommendations emphasize environmental redesign through attention to lighting arrangements, display techniques, interior design, exterior landscaping and control of parking patterns, aisle and customer-flow control, and management and employee training. Recommendations focus on changes in business procedures and physical plant modifications, rather than on installation of hardware devices or use of sentry personnel.

(P/D)

John W. Powell Consultants, Inc.
2600 Dixwell Avenue
Hamden, Connecticut 06514

Phone: (203) 248-2985

This firm specializes in the security problems of large, complex installations such as college and school campuses, utility and insurance companies, atomic power stations, business and industrial establishments, and computer centers. Assistance is also provided to architects in the planning and design of security systems and

programs for new facilities such as civic centers, large shopping/ office complexes, high-rise apartments, and condominiums. All services include analysis, study, recommendations for equipment and procedures, bid specifications, and training as required.

(G)

Profitect Inc.
Professional Protection Consultants
At Wharfside, 680 Beach Street
San Francisco, California 94109

Phone: (415) 283-3802
(415) 283-0511

(213) 786-4605 Los Angeles

This firm provides consultation for comprehensive protection programs, as well as systems and engineering guidance in equipment selection to architects, commerce, industry, hospitals, financial institutions, and data centers.

(C)

Protection Systems
10961 Bloomfield Street
Los Alamitos, California 90720

Phone: (213) 430-0786
(714) 826-0880

This firm offers security consultation and design work for public utilities, major shopping centers, large professional buildings, government agencies, state prisons, and police agencies, with some custom design of equipment. Specialties include: Design layout, installation, and maintenance of outdoor systems and access control, central alarms, and closed-circuit television.

(G)

Warner Consultants
75-A G Street, S. W.
Washington, D. C. 20024

Phone: (202) 737-0255

This company engages in research and development of security systems, which includes site evaluation system design and development.

The firm has carried out studies of this kind for industrial and commercial organizations, associations, and government agencies, emphasizing the effect of building design and location on security. Work has included developing a residential security planning and design guide and drafting a compendium of building concepts.

(C)

Westinghouse National Issues Center (WNIC)
2341 Jefferson Davis Highway
Suite 1111
Arlington, Virginia 22202

Phone: (202) 833-5959

The Westinghouse National Issues Center conducts studies on factors influencing criminal activity for governmental agencies; designs, assists in the implementation of, and evaluates demonstrations implementing crime prevention strategies; and provides consulting services to cities and authorities on crime prevention strategies in facilities design and operations. Demonstrations have been designed and implemented in such environments as schools, commercial/industrial, and residential. Typically, consulting on Crime Prevention Through Environmental Design (CPTED) techniques has been provided to a committee responsible for security design of a transportation/commercial/hotel complex, and to an authority responsible for redevelopment of an industrial area.

(G)

APPENDIX F

The Crime Prevention Through Environmental Design Program (CPTED)

1. INTRODUCTION

This appendix is intended to provide an understanding of the Crime Prevention Through Environmental Design concept. Such an attempt is a substantial undertaking, since CPTED is not an established discipline like police administration or corrections, but is simply a focus of concern. That concern derives from severely felt crime problems and represents an urgently required effort to provide alternative solutions for the prevention and reduction of crime. CPTED, as a crime prevention concept, is very much dependent upon the concepts and findings of behavioral science.

In brief, the CPTED approach focuses on the interaction between human behavior and the physical environment. It is hypothesized that the proper design and effective use of the environment can lead to reductions in crime and in the fear of crime. CPTED encompasses those strategies -- whether they be physical, social, management, or law enforcement in nature -- that affect, either directly or indirectly, criminal behavior or citizen response to criminal behavior. With respect to this study and the implementation of security considerations into the Navy Facilities Planning Cycle, the physical design concepts and strategies are of major concern and applicability.

2. THE CPTED PROGRAM

The primary goals of the CPTED Program are to reduce: (a) The incidence of common, predatory, stranger-to-stranger crimes; and (b) the public fear of such crimes. As a result of achieving the two primary goals, a third goal can be achieved: Improvement in the quality of life.

The goals of the CPTED Program are not novel; however, a new approach is presented for integrating and applying the insights of broadly based research on environmental design in a comprehensive way in three broad environmental modes (i.e., schools, residential, and commercial) with emphasis on certain Part I offenses (i.e., aggravated assault, robbery, burglary, larceny, auto theft).

Crime prevention strategies encompassed by the CPTED Program are not restricted to architectural design or redesign. Rather, the program seeks to combine a variety of anticrime resources (e.g., police, community groups, target-hardening strategies, social programs, and physical redesign) to create an environment minimally supportive of criminal activity. So stated, the goal of the program is not to alter criminal motivation directly (although indirect alteration may occur) but, rather, to intercede in its actualization: To prevent crime by placing obstacles in the way of the criminal objective.

3. CPTED CONCEPTS

The following sections describe four broad CPTED design concepts and related strategies for effecting their implementation. It is hypothesized that crime is prevented through strategies that foster certain types of access control, surveillance, activity support, and motivation reinforcement. These design concepts unavoidably overlap; in fact, a design strategy may reflect more than one design concept. Moreover, the same design strategy may reflect different design concepts when implemented in different environmental settings.

Some examples of strategies relative to the four design concepts are identified in Table F-1.

3.1 Access Control

Access control is primarily directed at decreasing criminal opportunity. In essence, it operates to keep unauthorized persons out of a particular locale if they do not have legitimate reasons for being there. In its most elementary form, some access control can be achieved in individual dwelling units or commercial establishments by use of adequate locks, doors, and the like (i.e., the group of design strategies known as target hardening).

However, when one moves beyond private property to public or semi-public spaces, the application of access control becomes more complicated. Lobbies of apartments, office buildings, or schools are often open to the public and, consequently, to some people willing to commit offenses if the opportunity arises. Of course, one strategy is to station guards at entrance points to screen visitors.

The problem is most acute on streets and similar areas that are entirely open to public use. In some areas, such as neighborhoods of tightly knit ethnic groups, the streets are effectively denied even to certain noncriminal outsiders by the imposition of social barriers. However, there are other, more legitimate techniques for limiting access in areas nominally open to the public. Physical barriers imposed by natural forms (e.g., rivers and lakes), existing manmade forms (e.g., railroad tracks, parks, vegetation, highways, and cemeteries), and artificial forms designed expressly as impediments (e.g., street closings and fences) serve to restrict movement.

Many burglars and robbers also display various environmental preferences, both physical and social, that can be frustrated by the creation of psychological barriers. These barriers may appear in the

TABLE F-1

Crime Prevention Through Environmental Design (CPTED)
Design Concepts and Illustrative Strategies

Strategy Component	Design Concepts			
	Access Control	Surveillance	Activity Support	Motivation Reinforcement
Physical	Provide protection in the form of target-hardening devices on the ground floor windows, entry points and skylights.	Provide adequate levels of lighting for pathways, entry points and parking lots. Eliminate visual barriers such as fences, shrubs and walls	Locate facilities which will attract users alongside pathways so as to generate activity, i.e., locate seating, recreation facilities or gardens near pathways.	Differentiate open grounds according to a hierarchy of public/semi-public/private zones through landscaping, different textured or colored paying materials, gateways.
Social	Organize, under law enforcement sponsorship, security forces who provide access control to major entry points	Organize programs where residents watch establishments which are temporarily vacant.	Engage teenagers in community maintenance services and recreational supervision.	Organize activities which foster a sense of community.
Law Enforcement	Employ off-duty law enforcement officials as security guards.	Increase police patrols in the target area.	Create substations to serve as base of operations on a localized, neighborhood scale for regular police activity.	Assign a special team to one area to integrate all patrol, traffic, community relations, and detective functions.
Institutional	Incorporate minimum security measures for access control into building codes.	Provide insurance rate reduction for increasing surveillance potential in and around insured buildings.	Zone for the integration land uses to generate activity.	Manipulate locations to create a greater socioeconomic integration.
Criminal Justice	Mandatory sentences for offenders convicted of illegal entry.	Use electronic surveillance measures to control illegal entry.	Involve criminal offenders in carefully supervised recreational and cultural activities outside prison walls.	Institute half-way houses, job training programs, and employment opportunities for rehabilitating criminal offenders.

form of signs, parkways, hedges -- in short, anything that announces the integrity and uniqueness of an area. The hypothesis operative in creating psychological barriers is that targets that seem alien, mysterious, or difficult may also seem unattractive to the potential offender. As a paradox, the hypothesis can work when areas -- by their clear legibility, transparency, and directness -- discourage the potential offender because of users' familiarity with each other and their surroundings, and the visible absence of places to hide or conduct furtive acts -- in short, because of the conspicuous cohesiveness of the area.

Because any strategy that fosters access control is also likely to impact upon egress, careful consideration should be given to access control strategies. Such strategies may not only limit the egress of offenders but also hinder the mobility of potential victims.

3.2 Surveillance

Although similar to access control in some respects, the primary aim of surveillance is not to keep intruders out (although it may have that effect) but, rather, to keep them under observation. Surveillance increases the perceived risk to offenders, and the actual risk if the observers are willing to act when potentially threatening situations develop. A distinction can be made between organized surveillance and natural or spontaneous surveillance.

3.2.1 Organized Surveillance

Organized surveillance is usually carried out by police patrol in an attempt to project a sense of omnipresence (i.e., to convey to potential offenders the impression that police surveillance is highly likely at any given location). The effectiveness of this particular technique may vary greatly with geographic considerations, temporal and crime-specific factors, and the efficiency of the police themselves. There is some evidence that community/police cooperation may be increasing spontaneously, and the spread of such indicators might prove a potentially important trend.

In some instances, surveillance can be achieved by nonhuman techniques such as closed-circuit television (CCTV) or alarms. Noteworthy success is reported to have been achieved in certain residential complex systems where the CCTV surveillance channel can be dialed on residents' individual sets; this medium provides an additional window on the world and even serves to promote social interaction. Better results might be achieved if the surveillance function of the CCTV

channel or channels were transformed or subordinated into one of several communications functions of the same system, so that crime surveillance could occur as a natural byproduct of a system actually serving several positive purposes.

3.2.2 Natural Surveillance

Natural surveillance can be achieved by a number of design techniques, such as channeling the flow of activity to put more observers near a potential crime area; or creating a greater observation capacity by such design directives as installing windows along the street side, enclosing a staircase in glass, or using single-loaded corridors. The technique of defining spaces can also convey a proprietary sense to legitimate users, inducing a territorial concern. At this juncture, the concept of surveillance overlaps with the design concept of (victim) motivation reinforcement (see Section 3.4).

3.3 Activity Support

The general design concept of activity support involves methods of reinforcing existing or new activities as a means of making effective use of the built environment. This design concept originates in the observation that in a given community, social and physical networks and nodes exist as latent, often underused, resources capable of sustaining constructive community activities. Support of these activities can bring a vital and coalescing improvement to a given community, along with a reduction of the vulnerable social and physical gaps that permit criminal intrusions. Such an approach might focus on a geographic area (e.g., block, neighborhood, city sector), a target population (e.g., vulnerable elderly victims, opportunistic youthful offenders), or an urban system (e.g., health delivery, transportation, zoning).

3.3.1 Incentives and Magnets

Increased community participation and related social interaction can result from the active design and provision of positive incentives or magnets that spur people to interact productively with each other, whether in the residential complex, the street, the neighborhood, or the city at large. If incentives and magnets exist for people to populate an area and to treat it as a semipublic extension of their own immediate habitat, they will use that area because it serves their personal needs and will also achieve the byproducts of natural surveillance, access control, and behavior reinforcement. Although activities and activity patterns appear to be the principal components of such incentives, they are also likely to include physical design manifestations.

A number of strategies can be employed to enhance the effective use of the built environment, such as: Reinforce existing, or encourage new, social networks; create activity magnets or nodes, especially those involving shared benefits; develop multipurpose centers that are used intensively; provide incentives for improving an area (and thereby raise the factors of territoriality, participation, and social interaction); and establish participatory goal- and priority-setting groups that carry out community programs of action (e.g., community development corporations).

3.3.2 Participation and Interaction

The complementary participation and interaction strategy emphasizes the important benefits that accrue when people coordinate and cooperate, thereby taking a share in process and product.

3.4 Motivation Reinforcement

In contrast to the more mechanical concepts of access control and surveillance that concentrate on making offenders' operations more difficult, motivation reinforcement seeks not only to affect offender behavior relative to the built environment but to affect offender motivation by increasing the risk of apprehension and by increasing the potential offenders' involvement in and identification with the physical and social environment that may be the object of criminal activity. Furthermore, this concept emphasizes positive reinforcement of the motivation of the nonoffender community (i.e., it functions to increase territorial concern, social cohesion, and general sense of security).

3.4.1 Offender

As it relates to the CPTED approach, behavioral science is in a developmental stage; the understanding of criminal motivation is still limited. Nevertheless, in terms of the CPTED Program, one might propose not only those strategies that indirectly affect the offender through the environment but also those that directly promote the transformation of human energy from illegal or destructive activity to legal or constructive outlets (including activity support strategies). These strategies, based on the maximization of positive human potentials, are supported by a growing body of theoretical and empirical studies, which seem appropriate for transfer to areas of CPTED concern.

For example, the Philadelphia Parkway School Program extends high school students' educational activity during and after school hours through work and study in the public and private facilities located in downtown Philadelphia. These activities include work/training programs in apprenticeship roles; special projects in the public museums, libraries, and recreation facilities; and a wide range of other constructive activities.

In an environmental sense, the Parkway School Program is an ingenious way of making better use of existing, but not optimally used, urban environmental resources on a large-scale multi-use basis. In a crime prevention sense, it is self-evident that potentially mischievous high school students engaged in learning a trade or performing a project will be prevented from participating in street crime. Similar programs in other modes could potentially involve other unproductive or excluded groups of the population.

3.4.2 Community

As stated previously, the motivation reinforcement concept also seeks to positively reinforce the motivation of potential victims, who constitute the nonoffender community. Territorial concern, social cohesion, and a general sense of security can result from such positive reinforcement strategies as altering the scale of a large, impersonal environment to create one that is smaller, more decentralized, and personalized. These results may also occur from improving its quality by such measures as upgrading the housing stock, the school facilities, or the interiors of subway cars; organizing occupants; or changing management policy. This last strategy may be very important, since citizen behavior in relation to an environment may not be so dependent on its physical aspects (such as architecture, land use, or location) as on its social relationships.

Territorial concern, social cohesion, and a general sense of security can be reinforced through the development of the identity and image of a community. Recognized consciously this approach can improve not only the image the population has of itself and its domain but also the projection of that image to others. With a definition and raising of standards and expectations, patterns of social estrangement decline, together with opportunities for aberrant or criminal behavior. CPTED application of this approach holds implications for the interaction of people and their built environment, especially by means of their participation in the physical upgrading and in the identity and image development of their territory.

4. CPTED STRATEGIES

4.1 General Strategies

As previously noted, the goal of the CPTED Program is to intercede in the actualization of criminal motivation by placing physical, social, management, and/or law enforcement obstacles in the way of the criminal objective. This section addresses the broad application of the access control, surveillance, activity support, and motivation reinforcement concepts, focusing on their conceptual application.

Concepts are general statements regarding the interaction between human behavior and the physical environment. They are rationales for development of specific design strategies which serve as the basis for developing the actual physical action required. For example, design strategies that are intended to deny access to a crime target are different in nature and effect from design strategies intended to keep offenders under observation (surveillance). Strategies are the means of utilizing these concepts to decrease criminal activity, and design changes are those strategies applied to a specific environment. The general thrust of a strategy may be physical, social, management- or law-enforcement-oriented, or frequently a combination of these. Design strategies are derived from and focus on specific crime-environment problems. Table F-2 shows examples of generic crime-environment problems, specific CPTED strategies, and design changes that could be applied to alleviate the problems.

4.2 Strategies in the Schools Environment

While the CPTED concepts described provide the basis for development of implementing strategies, it does not follow that a strategy, as applied in the real world, can support only one concept. In actual practice, a single strategy, such as relocating a parking lot, will increase natural surveillance, limit access of intruders, promote social interaction, and reinforce the users' motivation to maintain the area. Strategies, therefore, are developed based upon the problem defined, and make use of any or all of the concepts to achieve results. A better understanding of this process can be gained by considering the CPTED strategies developed for application in a controlled environment such as a county school system. These problem/strategy relationships are shown in Table F-3.

5. SUMMARY

The CPTED approach focuses on the interaction between human behavior and the physical environment. Its purpose is to develop concepts (and strategies) which will lead to the reduction of crime, and the public fear of crime. While this focus is broader than that of this study, which concentrates on the built environment and property losses, the concepts, and many of the strategies developed, are applicable. A knowledge of CPTED concepts and their application will assist in developing security engineering requirements.

Appendices A, B, C, and D show how CPTED concepts and strategies, as well as other presently used crime prevention practices, can be applied to the planning of design of facilities comparable to those of the Navy.

TABLE F-2

Crime Prevention Through Environmental Design (CPTED) Problems, Applicable Strategies, and Illustrative Design Changes
(Page 1 of 2)

CRIME-ENVIRONMENT PROBLEM	CPTED STRATEGIES	CPTED DESIGN CHANGES
Isolated and little-used corridors -- preemption of space by groups impeding traffic flow, producing confrontations and fear of assault. Areas are hard to supervise and are avoided by legitimate users, which increases isolation and lack of natural surveillance.	Provide clear definition of the dominant function (and intended use of space) and clearly define transitional zones to increase territorial concern and natural surveillance.	Place graphic designs in stairwells and corridors defining the intended function of these spaces.
		Color code various sections of the facility and use graphics and art designs uniquely for each functional component of the facility.
		Organize committees by functional component to select and coordinate the graphic design and color-coding activities.
	Provide a functional activity (or redesignate use) in blind spots or isolated areas to increase natural surveillance (or the perception thereof).	Relocate planning areas.
		Redesign blind spot areas to provide storage spaces for clubs and/or the administration.
	Remove obstacles to natural surveillance (increase perception of openness).	Install windows in walls of problem corridors.
		Install windows in walls of exterior stairwells.

TABLE F-2

Crime Prevention Through Environmental Design (CPTED) Problems, Applicable Strategies, and Illustrative Design Changes
(Page 2 of 2)

CRIME-ENVIRONMENT PROBLEM	CPTED STRATEGIES	CPTED DESIGN CHANGES
Breaking and entering, theft, and vandalism of autos due to poor design of parking lots.	Redesign parking lots to provide levels of security consistent with variable access needs.	Create a fenced parking area (secure) that is locked during the day.
		Create an open parking area (nonsecure) in a place with good natural surveillance.
		Assign parking to either the secure or nonsecure area on the basis of schedule.
		Reroute vehicular access to nonsecure parking area through internal parts of grounds before entering the parking lot.
		Set policy limiting pedestrian use of parking lot.
Fear of assault, robbery, or other crime in restrooms.	Remove obstacles to natural surveillance to decrease fear, to increase use and to increase the risk of detection.	Remove entrance doors to restrooms.
		Eliminate unnecessary portions of anteroom walls.
	Limit access to isolated areas during specific times for access control and to reduce the necessity for surveillance.	Install collapsible gates at restroom entrances for locking during problem periods.

TABLE F-3

Examples of Crime Prevention Through Environmental Design (CPTED) Problems, Related Strategies, and Design Changes for the Schools Environment
(Page 1 of 7)

CRIME-ENVIRONMENT PROBLEMS	CPTED STRATEGIES	CPTED DESIGN CHANGES
Design of and procedures for bus loading areas prohibit teacher surveillance, increase supervision ratio, impede pedestrian traffic flow and cause congestion. Confrontations, thefts and vandalisms occur.	Relocate and/or redesign bus-loading and parking lot access procedures to reduce necessity for pedestrian use of lot, reduce congestion in transitional zones and support strict definition of parking lot use.	Switch locations between student parking and driver education range.
		Designate access ways to the student parking lot and avoid the bus loading zone.
		Set policies to limit student pedestrian use of the parking lots.
		Require bus drivers to allow students to enter or leave their bus only when in a specified loading zone.
		Create a bus queuing zone for waiting buses that is convenient to the unloading zone.
		Require teachers on monitoring assignment at the bus loading zone to direct the movement of buses and to disperse each group of students from the bus loading area before allowing another group to load or unload.

TABLE F-3

Examples of Crime Prevention Through Environmental Design (CPTED) Problems, Related Strategies, and Design Changes for the Schools Environment
(Page 2 of 7)

CRIME-ENVIRONMENT PROBLEMS	CPTED STRATEGIES	CPTED DESIGN CHANGES
Design, use, and location of facilities has created isolated and blind spot areas that are difficult to survey (due to design and/or nonuse because of fear or avoidance). Assaults, thefts, and vandalism occur.	Provide functional activities in unused or misused problem areas to promote natural surveillance, increase safe traffic flow and to attract different types of users.	Create mini-plazas.
		Organize a student-faculty committee to assist in the design and coordination of mini-plaza activities.
Location of informal gathering areas (natural and designated) promotes the preemption of space, interferes with traffic flow and prohibits natural surveillance. Assaults occur.	Relocate informal gathering areas near supervision or natural surveillance.	Create mini-plazas or patios in the interior courtyard areas.
		Relocate the student smoking zone to the interior courtyards.
		Organize a student/faculty committee to assist in the design and coordination of the mini-plaza activities.
	Redesign informal gathering areas to promote orderly flow and break-up the preemption of space by groups.	Install new tables and benches that physically divide space and the size of groups (in the mini-plazas).
		Position amenities to create multiple access and passage ways (in the mini-plazas).
Provide clear border definition of transitional zones for access control and surveillance.	Provide clear border definition of transitional zones for access control and surveillance	Install low hedging, flower beds, or ornamental fencing along borders.

TABLE F-3

Examples of Crime Prevention Through Environmental Design (CPTED) Problems, Related Strategies, and Design Changes for the Schools Environment
(Page 3 of 7)

CRIME-ENVIRONMENT PROBLEMS	CPTED STRATEGIES	CPTED DESIGN CHANGES
		Organize a student/faculty committee to assist in the design and coordination of border definition activities.
Location and positioning of school physical plant prohibit natural surveillance (off hours) by local residents and passerbys. B & E, theft and vandalism occur. (One half of vandalisms are incident with B & E).	Provide functional community activities on school campus (off hours) to increase surveillance through effective use of facilities.	Create a police "school precinct" office.
	Overcome distance and isolation by improving communications to create rapid response to problems (and its perception) and more effective surveillance.	Install audio burglar alarm system.
Design, use and location of bicycle compounds or parking areas on school grounds prohibit natural surveillance and limit proper use because of students with variable hours. Thefts of bicycles occur.	Redesign bicycle parking areas to provide levels of security consistent with variable access needs of students.	Create a fenced bicycle parking area (secure area).
		Create an open bicycle parking area located in a place with good natural surveillance (nonsecure area).
		Install ground level locking devices in each bicycle locking cable or chain.
		Assign bicycle students to either secure or nonsecure parking area on the basis of schedule.

TABLE F-3

Examples of Crime Prevention Through Environmental Design (CPTED) Problems, Related Strategies, and Design Changes for the Schools Environment
(Page 4 of 7)

CRIME-ENVIRONMENT PROBLEMS	CPTED STRATEGIES	CPTED DESIGN CHANGES
Design and location of parking lots provide unclear definition of transitional zones and unmanaged access by vehicles and pedestrians, students and nonstudents. B & E, thefts and vandalisms occur. (Trespassing also).	Provide natural border definition and limit access to vehicular traffic in student parking to clearly define transitional zones, to reroute ingress and egress during specified periods and to provide natural surveillance.	Install hedges around parking lots.
		Install aesthetically pleasing gates at vehicular access points.
		Set policies to limit student pedestrian use of the parking lots.
		Secure gates at external vehicular access points during school hours, leave internal access points open.
		Organize a student/faculty committee to assist in the design and coordination of the border definition and parking lot access control activities.
Design and use of corridors provide blind spots and isolated areas that prohibit natural surveillance. Assaults, threats and extortions occur.	Provide a functional activity (or redesignate use) in blind spots or isolated areas to increase natural surveillance (or the perception thereof).	Relocate a teacher planning area to the space under one of the interior stairwells.
		Redesign blind spot areas to provide storage spaces for clubs and/or the school administration.

TABLE F-3

Examples of Crime Prevention Through Environmental Design (CPTED) Problems, Related Strategies, and Design Changes for the Schools Environment
(Page 5 of 7)

CRIME-ENVIRONMENT PROBLEMS	CPTED STRATEGIES	CPTED DESIGN CHANGES
	Remove obstacles to natural surveillance (increase perception of openness).	Install windows in walls of problem corridors.
		Install windows in walls of exterior stairwells.
Class scheduling promotes congestion in certain areas at shift changing that decreases supervision capabilities and produces inconvenience. Assaults and confrontations occur.	Revise class scheduling and management procedures to avoid congestion, to decrease supervision ratio and to define time transitions.	Provide a 3-5 minute shift change "hiatus" between lunch periods.
Location of benches and/or other amenities in corridors creates misused space and congestion. Corridor locations are lacking in natural surveillance because of design. Assaults and confrontations occur.	Relocate informal gathering areas to areas with natural surveillance and that are designed to support that activity.	Remove benches and other physical amenities from crowded corridors.
Location and use of corridors for functions other than pedestrian passage such as smoking zones promotes preemption of space by groups and unsurveillable misused space. This misused space supports behavior that attracts outsiders to the external corridors designated as smoking areas. Assaults, confrontations and other illegal activity occur.	Relocate activities and functions from misused space to areas designed to support these activities and to provide natural surveillance.	Provide cafeteria food at gymnasium snack bar.
		Provide multiple access to the snack bar and queuing lanes.
		Move the existing student smoking zones from corridors to mini-plazas.

TABLE F-3

Examples of Crime Prevention Through Environmental Design (CPTED) Problems, Related Strategies, and Design Changes for the Schools Environment
(Page 6 of 7)

CRIME-ENVIRONMENT PROBLEMS	CPTED STRATEGIES	CPTED DESIGN CHANGES
		Revise school policy to restrict student use of the outside corridor previously designated for smoking.
Design and definition of corridor areas do not support a clear definition of the dominant function of that space (i.e., passage). Unclear transitional zones produce behaviors conducive to assault and confrontation.	Provide clear definition of the dominant function (and intended use of space) and clearly define transitional zones to increase territorial concerns and natural surveillance.	Place graphic designs in corridor defining the intended function of this space.
Location of restrooms near external entrances and exits isolates them from normal school hour traffic flow and prohibits surveillance. Assaults occur.	Limit access to isolated areas during specific times for access control and to reduce the need for surveillance.	Install collapsible gates at restroom entrances for locking during problem periods.
Privacy and isolation required for internal design provides blind spots that reduce surveillability on the part of students and supervisory personnel, i.e., exterior door and anteroom wall. Assaults occur.	Remove obstacles to natural surveillance to decrease fear, increase use and increase risk of detection.	Remove entrance doors to restrooms.
		Eliminate unnecessary portions of anteroom walls.

TABLE F-3

Examples of Crime Prevention Through Environmental Design (CPTED) Problems, Related Strategies, and Design Changes for the Schools Environment
(Page 7 of 7)

CRIME-ENVIRONMENT PROBLEMS	CPTED STRATEGIES	CPTED DESIGN CHANGES
Design requirements for classrooms produce isolation of individual classes, resulting in high student to teacher ratios and little external natural surveillance (real or perceived) when class is in session. Assaults occur. (Thefts occur when class is empty).	Remove obstacles to natural surveillance to increase risk of detection and to reduce perception of isolation.	Install windows in classroom walls and doors.
	Overcome distance and isolation by improving communications to create rapid response to problems, the perception of rapid response, and more effective surveillance.	Provide portable radios to deans, school resource persons, and custodial personnel.
		Install audio alarm systems in problem classroons for after hours.
Location and design definition of multiple purpose classrooms produces unclear transitional zones, decreases territorial concern, and decreases natural surveillance. Thefts occur.	Extend the identity of surrounding spaces to multiple purpose space to increase territorial concern and natural surveillance.	Color-code and graphically identify multiple-purpose classrooms with adjacent spaces.
	Provide a functional activity in problem areas to increase territorial concern and natural surveillance.	
Class shift procedures during lunch hour produce unclear time transition and definition of groups; decrease control and increases student to teacher ratio (many classroom thefts are committed by classcutters).	Revise class scheduling and movement procedures to define time for class shifts making surveillance and supervision of classcutters easier.	Provide a 3-5 minute shift change "hiatus" between lunch periods.

APPENDIX G

Annotated Bibliography

This appendix is a selected bibliography of source materials that address environmental and industrial security, particularly as they relate to the planning, design, and construction of new facilities and industrial complexes similar to those operated by the Navy.

The entries are presented alphabetically by corporate author and are indexed by subject, title, and individual author.

1. Alexander, Alfred, and Val Moolman. Stealing. New York, NY: Cornerstone Library Publications, 1969.

This is a guidebook for management personnel on how to reduce their losses by bringing the incidence of pilferage under control. This book exposes the tricks of thieves and provides management with tips on how to beat the game.

2. Berla, N. The Impact of Street Lighting on Crime and Traffic Accidents, Library of Congress Legislative Reference Service, Washington, DC, 1965.

The article surveys the findings of studies performed in various U.S. cities and concludes that fewer crimes and street accidents followed a significant increase in the level of street illumination.

3. Blanchard, Janelle. "Proposal for a Model Residential Building Security Code," p. 1-25. In U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Deterrence of Crime In and Around Residences.

Deals with the physical design elements that might be incorporated into building codes as a means of residential crime prevention. Emphasizes the need for uniform building codes to improve industrialized housing, but states that security codes must recognize differing needs.

4. Brill, W. H. "Security in Public Housing: A Synergistic Approach," p. 26-43. In U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Deterrence of Crime In and Around Residences.

Looks toward a mix of project security improvements, including target hardening approaches and measures to increase the social cohesion of the residents, which together would produce a synergistic effect. Mentions the Innovative Modernization Project (IMP), in which were tested and evaluated ways to improve the quality of life in public housing.

5. California. Council on Criminal Justice. Selected Crime Prevention Programs in California. Sacramento, CA: Council on Criminal Justice, 1973.

Reports on crime prevention programs in use in California that focus on action that can be taken before crimes occur, based

on questionnaires and a series of onsite visits to 172 law enforcement departments. Included are the program's purpose, past results, recommended implementing procedure, possible problem areas, costs, and recommended forms and literature. Reviews programs dealing with areas such as crime prevention units, facility planning, property identification, residential, commercial, and industrial security inspections, and commercial robbery prevention.

6. _____. Department of Justice. "On the Alert! How to Protect Your Business and Property," California Department of Justice Information Pamphlet No. 4, prepared by Evelle J. Younger, Attorney General, August 1973.

This pamphlet briefly discusses how businessmen can guard against shoplifting, employee theft, bad checks, robbery, and burglary in new and existing facilities. Site selection, building placement, parking, perimeter controls, lighting, and traffic flow all are cited as important considerations.

7. _____. Department of Justice, Attorney General's Building Security Commission. Building Security Standards -- Preliminary Report to the California Legislature. Sacramento, CA: Department of Justice, January 1973.

Defines the problem of creating and maintaining physical security and establishes a logical approach for developing building security standards. Concentrates on the physical aspects of elements in barrier systems, with emphasis on window and door elements as being the most frequently attacked.

8. _____. University. Space Sciences Laboratory and Center for Planning and Development Research. Discouraging Crime Through City Planning, by Shlomo Angel. Prepared for the National Aeronautics and Space Administration. Working Paper No. 75. Berkeley, CA: University of California, February 1968.

The author proposes that environmental prevention can forestall crime, and focuses on the characteristics of areas where crime occurs. He hypothesizes that crime is a function of opportunism, and that areas of high-crime density are typically easily accessible to and well known by the criminal, are known to offer high likelihood of finding a victim at a given time, and involve little risk of police apprehension. With emphasis on intensity of use as a major factor in crime occurrence and the hypothesis of a critical use intensity zone, the author suggests

adjustment of intensities of pedestrian circulation channels as an environmental design solution. By means of 13 alternative design configurations, he indicates how specialized activity areas like industrial areas can be evaluated at night, evening establishments centralized, and strip commercial developments altered to either decrease or increase intensity of use so as to avoid the critical high-crime intensity zone.

9. Cedar Rapids, Iowa. Police Department. Installation, Test, and Evaluation of a Large-Scale Burglar Alarm System for a Municipal Police Department -- Second Phase Completion Report. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. Cedar Rapids, IA: Cedar Rapids Police Department, December 1971.

   Describes the effectiveness of a simple and inexpensive central station burglar alarm system installed under police supervision in 350 businesses in Cedar Rapids. Interim results from the program indicate that the alarms are effective in improving police arrest and clearance figures, but not necessarily effective in deterring burglars.

10. Center for Residential Security Design. Design Directives for Achieving Defensible Space, by Oscar Newman. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. New York, NY: Center for Residential Security Design, June 1973.

    This is a handbook for housing officials, architects, and urban planners. Gives instructions for providing residential security through employment of hardware and security personnel, and is directed toward the initial design and programming of new residential developments. Discusses building codes and the problems the present code structure creates in providing security.

11. Cherico, P. "Security Requirements and Standards for Nuclear Power Plants," Security Management, 18(6): 22-24, January 1975.

    Reviews present and proposed security requirements to protect against acts of sabotage and against the diversion and misuse of special nuclear materials. The present requirements of the Atomic Energy Commission and the American National Standards Institute are examined. Among the areas covered in these standards are the use of a physical security plan, security guards, alarm systems, and general security systems.

Projected requirements in the areas of materials and plant protection, personnel selection, training, and access control also are discussed.

12. Colling, Russell L. Hospital Security: Complete Protection for Health Care Facilities. Culver City, CA: Security World Publishing Co., Inc., 1976.

    This book examines the entire field of health care protection, developing a detailed, practical program for establishing a security system or refining existing programs. Hospital vulnerabilities and the security function are analyzed in depth, including security administration and operations, preventive programming, emergency operations, and special problems. Such diverse areas as hiring and training, records and reports, psychological deterrents, disaster planning, and drugs and pharmacy controls are covered. The information presented is intended to bring to top level management a basic understanding of protection needs, provide the security administrator with operational guidelines and practical program suggestions, and give the line officer and supervisor a background which will enable them to better understand health care security systems and their interaction within the operational program. A subject index is included.

13. Cooper, Clare. "St. Francis Square: Attitudes of Its Residents," AIA Journal, 56(6): 22-27, December 1971.

    Treats the effect of environmental design on attitudes of residents of a city housing project, and provides an example of the apparently successful incorporation of "territorial" design principles in housing projects.

14. "Cost of Crimes Against Business," Security Management, 19(1): 6-14, March 1975.

    Summary of the available knowledge of industry and the Federal government on the extent of the dollar loss of American business to crime in the period since 1971. Discussed individually are: Bad checks, counterfeiting, inventory shortages, robbery, vandalism, and other crime-related problems. Crime prevention measures are outlined.

15. Dillingham Corporation. SUA Division. A Study of Crime Prevention Through Physical Planning. Prepared for Southern California Association of Governments. Los Angeles, CA: Dillingham Corporation, September 17, 1971.

Provides information on existing or proposed techniques for achieving security in future residential, commercial, industrial, institutional, and recreational developments through the manipulation of the physical characteristics of these developments. Focuses on the planning of future developments, and urges that similar efforts be directed toward modification of existing structures.

16. Educational Facilities Laboratories, Inc. Designing Schools to Minimize Damage from Vandalism and Normal Rough Play. Schoolhouse Newsletter No. 15. New York, NY: Educational Facilities Laboratories, Inc., 1974.

Based upon a study conducted by Professor John Zeisel, Graduate School of Design, Harvard University. Briefly describes four categories of vandalism and suggests possible design responses to minimize the burden of cost resulting from vandalistic activities.

17. Educational Resources Information Center. ERIC Clearinghouse on Educational Management. School Security, by Nan Coppock. Educational Management Review Series No. 23. Eugene, OR: University of Oregon, October 1973.

Explores briefly the general dimension of crime in public schools, inventories the types of antivandalism techniques in current use, and cites data on the incidence of crimes against persons occurring in schools.

18. Fireman's Fund Insurance Company. Protecting Your Business from Embezzlement, Burglary, and Robbery. San Francisco, CA: Fireman's Fund Insurance Company (P.O. Box 3395, San Francisco, CA 94119).

This booklet outlines conditions or actions that facilitate crimes against businesses and offers several countermeasures. Discussed are problems of internal security; control of vulnerable areas such as receivables, purchases, and inventories; physical security; and mechanical crime prevention methods.

19. Fortune, Thomas. "Schools Equipped with 'Ears' to Fight Vandalism," Los Angeles Times, September 5, 1973.

Describes a sound monitoring intrusion alarm system being installed in the Placentin, Orange, and Santa Ana unified

school districts to prevent vandalism and burglary. The commercially available system utilizes a public address speaker that is set to trip a light at police headquarters when noise exceeds a predetermined level, allowing the dispatcher to listen in on whatever triggered the alarm.

20. Gocke, B. W. Practical Plant Protection and Policing for the Security of Business and Industry. Springfield, IL: Charles C. Thomas, 1957.

Studies the requirements for effective, efficient business and industrial security protection and recommends methods of application. Provides a working basis for increased profits by virtually all types of enterprises by analyzing factors involved in the physical security of facilities (e.g., access control).

21. Griffin, R. K. "Theft Against Retail Profit: A Management Perspective," Security World, 9(4): 14-15, 17-20, April 1972.

Guidelines for evaluating the cost of shoplifting, curbing employee theft, and involving employees in theft prevention programs.

22. GTE Sylvania Incorporated. Security Systems Department. An Evaluation of Small Business and Residential Alarm Systems, by T. P. Chleboun and K. M. Duvall. 2 v. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration. M-1442. Mountain View, CA: GTE Sylvania Incorporated, June 1972.

Presents a comprehensive discussion of the role of various alarm systems, including information about offenders and an analysis of the crime risk characteristics of various categories of alarm users. Evaluates alarm systems in terms of "threat probability," and presents a shopping list of applicable equipment. Provides offender and victim profiles, correlated with variations on a particular crime deterrent (alarm system).

23. Healy, R. J. Design for Security. New York, NY: Wiley, 1968.

Analyzes the optimum security layout for industrial facilities, starting with the premise that security can, at best, provide only physical controls that act as "impediments to the undetermined." In the context of this book, security is intended not only as protection against common-law crimes such as theft but also against industrial espionage and sabotage.

24. Hemphill, C. F., Jr. Security for Business and Industry. Homewood, IL: Dow Jones-Irwin, 1971.

Methods for reducing business losses due to theft, vandalism, fire, burglary, embezzlement, and other problems. Discusses physical aspects of business security from the selection of plant location and actual building of the plant to an assortment of alarm devices and protective services. Sound procedural controls are detailed, which apply to purchasing and receiving, warehousing and stockkeeping, shipping and deliveries, control of merchandise in sales areas, and the handling of cash receipts.

25. Holcomb, R. L. Protection Against Burglary. Iowa City, IA: State University of Iowa Institute of Public Affairs, 1973.

Describes to potential victims the things they can do to thwart burglars and to reduce their losses in the event of burglary. Concludes with surveys for use in commercial buildings and residences.

26. Hughes, M. M. (ed). Successful Retail Security: An Anthology. Los Angeles, CA: Security World Publishing, 1973.

Presents articles (reprinted from the professional security magazine, Security World) on methods and programs that retailers have used to counter a broad range of crimes and other hazards.

27. Jacobs, Jane. The Death and Life of Great American Cities. New York, NY: Vintage Books, 1961.

Attacks the current city planning procedures of functional separation of types of land use. Maintains that, in designing new urban environments, planners ignore the most basic structure of the city -- the intricate and closely connected diversity of uses that constantly reinforce one another economically and socially.

28. Kentucky. University. College of Engineering. Office of Research and Engineering Services. Proceedings of the 1973 Carnahan Conference on Electronic Crime Countermeasures, Lexington, Kentucky, May 1-3, 1972. Compiled by J. S. Jackson and R. W. DeVore. Prepared in cooperation with the Institute of Electrical and Electronics Engineers. Lexington, KY: University of Kentucky, 1973.

Presents a compendium of papers on the design and application of various electronic surveillance, alarm, and information processing systems.

29. Kingsbury, A. A. Introduction to Security and Crime Prevention Surveys. Springfield, IL: Charles C. Thomas, 1973.

    Provides a reference text for police officers, professional security consultants, and college-level students of security. Offers step-by-step guidelines for conducting onsite examination and analysis of premises to identify physical opportunities for crime and to develop methods for reducing such opportunities.

30. Knight, P. E., and A. M. Richardson. The Scope and Limitation of Industrial Security. Springfield, IL: Charles C. Thomas, 1963.

    The authors examine the reasons for and purpose of industrial security, defining its nature and limitations both in general and in reference to various professional methods, operations, and mechanics.

31. Kwan, Q. Y. Scope, Nature, and Prevention of Vandalism. Prepared for the U.S. Department of Justice. Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, 1972.

    Short- and long-range approaches to the problem of vandalism are proposed. Architectural and environmental design considerations figure prominently in short-range proposals. Some suggestions are unbreakable glass, fenceless parks, well-lighted public areas, and concrete-encased plumbing fixtures.

32. Liechenstein, Michael. Designing for Security. Paper presented at the American Institute of Aeronautics and Astronautics Urban Technology Conference, New York, N.Y., May 24-26, 1971. P-4633. New York, NY: The Rand Corporation, (n.d.).

    Suggests the need for cooperation among architects, security experts, social psychologists, and government agencies during the planning phases of new buildings. Critical to crime prevention is the demarcation, arrangement, and hierarchy of public and private areas at the

building conception. The high post-construction costs of implementing security measures are stressed, as is the benefit of multifunctional integrated design units providing fire, burglary, robbery, and utility protection.

33. Loss Prevention Diagnostics, Inc. Three Solutions in Reduction of Criminal Opportunity in Mass Transportation. A Selection of Devices and Techniques to be Demonstrated in Mass Transportation. Prepared for City of Chicago, Department of Public Works, Transit Security Study. Caldwell, NJ: Loss Prevention Diagnostics, Inc., June 15, 1973.

    Presents in detail three solutions developed for Chicago Transit Security project. Gives potential implementation sites, hardware requirements and possible suppliers, and estimated costs for each of these solutions. Also describes modified construction and lighting to enhance surveillance.

34. Luedtke (Gerald) and Associates. Crime and the Physical City, by Gerald Luedtke et al. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. Detroit, MI: Gerald Luedtke and Associates, 1970.

    Analyzes the importance of selected physical features to the crimes of robbery and burglary, including the conditions and maintenance of buildings, streets and alleys, lighting, mixtures of land use, rates of pedestrian flow, landscaping, visibility of entrance and exit points. The data base used is an inventory of physical features in 289 structures in which crimes have been recorded by the Detroit Police Department.

35. Malt (Harold Lewis) Associates, Inc. Tactical Analysis of Street Crimes, by H. L. Malt et al. Prepared for City of Jacksonville, Fla., Office of the Sheriff. Washington, DC: Harold Lewis Malt Associates, Inc., 1973.

    Examines the relationship between the physical street environment and street crime, specifically whether certain environmental indicators (e.g., bushes, abandoned buildings) affect the location and incidence of street crime; whether users, offenders, and policemen are aware of this effect; and whether their behavior is influenced by their perception of the environmental indicators.

36. Mandlebaum, A. J. Fundamentals of Protective Systems: Planning/Evaluation/Selection. Springfield, IL: Charles C. Thomas, 1973.

Provides a basic survey and comparative evaluation of the protective systems currently available to both business establishments and private systems. Emphasizes security devices as opposed to design factors.

37. Maurer, E. C. "Housing Project Safety Restored," Journal of Housing, 28(6): 282, June 1971.

Indicates that lighting proved effective in one housing project in reducing vandalism, muggings, and other crimes.

38. Michigan. University. Impact of Street Lighting on Street Crime, by Roger Wright, et al. 2 v. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. Ann Arbor, MI: University of Michigan, May 1974.

Describes an investigation of the crime deterrent effects of upgrading street lighting from incandescent to mercury and sodium vapor in selected high-crime commercial and residential areas in Kansas City, Missouri. The two areas are commercial, located in the central core, and residential, in an adjacent zone. Effectiveness is assessed by comparing changes in crime rates before and after installation in both relit and nonrelit areas. Crimes of violence are significantly deterred, while crimes against property are largely unaffected.

39. Moolman, V. Practical Ways to Prevent Burglary and Illegal Entry. New York, NY: Cornerstone Library, 1970.

Various modi operandi of burglars, with concise and practical descriptions of security hardware and measures for burglary protection and prevention. Aspects of security ranging from architectural design to effective use of lighting are discussed. The designs and operations of locking devices are described along with recommendations for their proper use. The different types of alarm systems are explained. Theft prevention measures covered include applications to residential, commercial, and automobile security.

40. Morse, G. P. Protecting the Health Care Facility: A System of Loss Prevention Management Effective for All Industry. Baltimore, MD: Williams and Wilkins Company, 1974.

The responsibility for security and protection of property and persons is considered to be that of the management. The procedure for developing and implementing a protection plan is presented. Accident prevention, fire prevention, radiation safety, asset protection, and personnel protection are discussed. Access control, data processing, key control and masterkeying, parking administration, and construction review are identified as important procedures for reducing loss and accidents.

41. Murphy, H. J. "Security of Airport Parking Lots," Security Management, 19(2): 22-25, May 1975.

This article discusses the physical security of airport parking lots in particular, based on principles that have been used and proved effective in industrial, educational, and health facilities. Emphasis is on designing security into the lot to eliminate targets of opportunity and prevent or deter criminal activity. This is achieved through a combination of design techniques and human cooperation.

42. Murphy, Ralph. "Design for Physical Security," Security Management, 20(20): 12, 14, March 1976.

In this article, the author emphasizes that "the most effective way... in establishing operational security requirements is in the new construction stage, 'before' the design is accepted and becomes firm." Based on this, general architectural/security considerations are discussed (e.g., access control, traffic flow), as well as some specific strategies to achieve desired results.

43. Murphy, Ralph, and William Norman. "Physical Security: Chance, Choice, Change," Security Management, 20(2): 8-10, March 1976.

This article defines physical security and discusses applications through deterrent, interior, and internal protection. For example, the authors cite that criminal activity can be deterred through "Proper design or configuration changes in a facility's perimeter, lighting changes ..."

44. "Need for Security in Buildings More Demanding," Engineering News Record, 189(11): 25-33, September 14, 1972.

Discusses hardware countermeasures to crimes in office and residential buildings.

45. New Mexico. University. Institute for Social Research and Development. Transfer Potential of Crime-Specific Programs to Metropolitan Albuquerque, by G. S. Metarelis. Prepared for U.S. Department of Justice, Law Enforcement Assistance Administration. Albuquerque, NM: University of New Mexico, November 1972.

Discusses recent techniques used to counter crime, and describes crime prevention programs in seven large cities with respect to methods and results. Includes model building-security ordinances for Seattle and Oakland.

46. New York, New York. Street and Highway Safety Lighting Bureau. Out of the Shadows. New York, NY: New York, (n.d.)

Shows how street lighting can help reduce crime and traffic accidents.

47. New York City Rand Institute. Improving Public Safety in Urban Apartment Dwellings: Security Concepts and Experimental Design for New York City Housing Authority Buildings, by William Fairley and Michael Liechenstein. R-655-NYC. New York, NY: The Rand Corporation, June 1971.

Addresses the reduction of crime in the New York City Housing Authority's existing public housing facilities. The three crimes of particular interest are vandalism, robbery, and burglary. The purposes of this project are to define the problem and security alternatives, develop guidelines for estimating the cost effectiveness of security alternatives, and develop experimental models to evaluate the estimated effectiveness of different security measures.

48. Newman, Oscar. "Architectural Design for Crime Prevention," p. 52. In U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Deterrence of Crime In and Around Residences.

Describes defensible space as a form of crime prevention that, while basically mechanical, also acted as a form of corrective prevention, alleviating some of the causes of criminal behavior.

49. _____. Defensible Space: Crime Prevention Through Urban Design. New York, NY: Macmillan, 1972.

Develops the concept of residential security predicated on a positive correlation between architectural design and behavior. While the author does not claim that design can mandate behavior, he posits that the forms of an environment can elicit responses from the inhabitant of that environment that can enhance his security. On the simplest level, architects can create or prevent encounters. Latent attitudes of territoriality, the acknowledgment that a space is a domain that warrants protection, and the increased awareness of "spheres of influence" on the part of the young will operate to inhibit crime both "mechanically" and "correctively." This territoriality, fostered by physical means -- grouping dwellings in a residential complex, defining and differentiating grounds, providing means for natural surveillance, positioning routes -- is essential to a self-defending community. Crime is deterred when the easy opportunity to vandalize, rob, burglarize, or rape is thwarted by the territorial prerogative of residents.

50. Panhandle Regional Planning Commission. A Study of Building Codes as Related to Crime Prevention, by Peat, Marwick, Mitchell and Company. Prepared for U.S. Department of Housing and Urban Development, and for Texas Criminal Justice Council. Amarillo, TX: Panhandle Regional Planning Commission, September 1972.

This document is the report of a HUD/Texas Criminal Justice Council pilot study to determine the relationship between building codes and crime prevention. Part I presents a general survey of trends of burglary and related offenses nationwide and in the Panhandle area. In Part II, the findings to date of research programs in the field are summarized.

51. Post, R. S., and A. A. Kingsbury. Security Administration -- An Introduction. Springfield, IL: Charles C. Thomas, 1973.

Presents an introductory text on the background, components, and programming of government and proprietary security activity for security and law enforcement personnel.

52. Salama, Ovadia, and Alexander Tzonis. "Strategies for Defense," Progressive Architecture, (4): 72-75, April 1974.

Describes the development of a framework for generating crime-reducing features in a variety of environments and transferring Newman's findings from the area of public housing to other environments.

53. San Luis, Edward. Office and Office Building Security. Los Angeles, CA: Security World Publishing, 1973.

Discusses those areas most likely to be identified as criminal activity (i.e., burglary, robbery, arson, violence, and industrial espionage). Evaluates security techniques that have proven most successful in identifying and defending against problem areas quickly and efficiently.

54. Sears, H. Crime, Vandalism, and Design. Paper presented at the Crime Prevention Workshop held at the University of Toronto, Centre of Criminology, May 20-22, 1975. Toronto, Ontario, Canada: University of Toronto, Centre of Criminology, 1975.

Examines background information on the relationship of crime and environmental design, and explores the means by which physical environments can be designed and modified to reduce vandalism and crime. It is noted that such building features as impersonal spaces, lack of needed facilities, overcrowding, and unsurveillable spaces promote crime and vandalism.

55. Sommer, Robert. Personal Space: The Behavioral Basis of Design. Englewood Cliffs, NJ: Prentice-Hall, 1969.

Discusses the psychology of designing space. The basic premise is that spatial relationships affect user behavior in a quantifiable fashion and in other more complex and less measurable ways. The treatment is philosophical and speculative; however, specific studies of the effect of spatial arrangements on social interaction are described.

56. Southern California Association of Governments. Handbook of Crime Prevention Bulletins: Crime Prevention Through Physical Planning. Los Angeles, CA: Southern California Association of Governments, 1971.

Draft of 16 single-topic bulletins that provide information on how to prevent crime through the planning and design of physical characteristics and their application to specific projects, such as apartment complexes, industrial parks, commercial recreation developments, and public buildings.

57. Thornsen, J. E. "Air Cargo Security: A Concept that Works," Security World, 10(6): 28-31, 34-35, June 1973.

This article discusses the security problems of an air freight company and procedures, electronic devices, and systems used to reduce loss at Kennedy Airport in New York, and describes the security measures undertaken to reduce overall losses from freight damage and theft. Reports on the security actions taken to reduce opportunity for snatch-and-run thievery, forgery, or pilferage. Procedures described include the architectural redesign of space to enable cargo containment and clear observation, the installation of closed circuit television at key points, the systematic recording and tracing of cargo throughout the process, the required use of a special stamp to guarantee pickup authority, and the tightened processing of truckers making pickups. The handling of sensitive merchandise using a special security cage is also described. Dramatic reduction in loss was reported.

58. Tyska, L. A. "Security Lighting for the Cargo Terminal," Security Management, 20(3): 40-41, July 1976.

This article, which is based on the premise that use of lighting is an effective deterrent to criminal activity, discusses what proper and adequate lighting is. Discussed are recommended light levels and location points.

59. U. S. Congress. Senate. Crime Against Small Business. A Report of the Small Business Administration Transmitted to the Select Committee on Small Business. S. Rept. 91-14, 91st Congress, 1st Session, 1969.

Provides a benchmark of current problems and solutions to crime, so as to encourage optimum use of existing crime prevention measures (particularly, protective devices, architectural design, and managerial systems) and to encourage the provision of more effective crime insurance. The main orientation of the study is specifically the small businessman and real-world remedies on a cost/benefits basis.

60. U. S. Department of Housing and Urban Development. Office of Policy Development and Research. Division of Building Technology. A Design Guide for Improving Residential Security, by Oscar Newman; Center for Residential Security. HUD Guideline 2. Washington, DC: Government Printing Office, December 1973.

Presents the thesis that a well-designed residential security system is one with a functioning interrelationship between the various component parts. Each element is examined in separate chapters. This text directs its attention primarily to the creation of fortifications because, "it is the easiest to implement after the act of building is completed, whereas defensible space concepts are best achieved in a project's inception."

61. U. S. Department of Justice. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Architectural Design for Crime Prevention, by Oscar Newman; New York University, Institute of Planning and Housing. Washington, DC: Government Printing Office, March 1973.

Updates the observations on environmental design originally presented in Newman's Defensible Space (q.v.). Discusses the concept of "defensible space" and human territorial instincts, and reviews the works of other authors, as they relate to defensible space. Relies heavily on pictorial rather than tabular presentation.

62. _____. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Minimum Building Security Guidelines and Cost Estimate for the Security Features. Initial Draft. Prepared in Cooperation with the Federal Insurance Administration, Department of Housing and Urban Development. Washington, DC: Department of Justice, May 14, 1971.

Contains a model security code covering minimun standards for doors, windows, safes, and alarms for commercial and residential buildings. Standards are expressed largely in design rather than performance factors.

63. _____. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Urban Design, Security and Crime. Proceedings of a Seminar in Washington, D. C., April 12-13, 1972. Compiled by R. M. Rau. Washington, DC: Department of Justice, January 1973.

Focuses on security measures for preventing burglary and stranger-to-stranger crimes in and around residences and businesses in the urban community. Reviews the state-of-the-art, and develops proposed research and action ideas for the future.

64. _____. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Law Enforcement Standards Program. Directory of Security Consultants, by Elizabeth Robertson and John V. Fechter; Center for Consumer Products Technology, National Bureau of Standards, Washington, DC: Government Printing Office, October 1975.

This is a directory of security consultants available to assist the consumer in solving security problems. The resources listed in this document should be of help to the general public, community authorities, police, businesses, and others wishing to identify known and effective strategies to eliminate or protect targets of opportunity, in addition to identifying measures and mechanisms to stimulate community support of such strategies. While the scope of this directory is limited primarily to targets of opportunity, the protection of high security targets is within the competence of some of the individual resources that are listed.

65. U. S. Department of the Army. Physical Security. FM 19-30. Washington, DC: Department of the Army Headquarters, February 17, 1965.

Presents material that is applicable to the security problems of both military and industrial installations. Includes a physical security checklist.

66. U. S. Department of Transportation, Office of the Secretary. Guidelines for the Physical Security of Cargo. Washington, DC, May 1972.

Presents guidelines to assist transportation management in stemming the over-$1-billion annual loss due to cargo theft and pilferage. Because analysis of these problems revealed that 85 percent of cargo stolen is removed by authorized persons or vehicles, the guidelines are directed towards methods against internal threats.

67. Ursic, H. S., and L. E. Pagano. Security Management Systems. Springfield, IL: Charles C. Thomas, 1974.

Establishes a systems approach to organizational security management. Emphasis is on a total (viewing the organizational entity as a whole) and open (to society) systems approach to the management functions related to the organizational function of security. Organizational security is

defined as a service function whose purpose is to develop a social awareness for the protection of life and property within private and public institutions as a collective responsibility complementing law enforcement.

68. Walsh, T. J., and R. J. Healy. Protection of Assets Manual. Santa Monica, CA: The Merritt Company, 1975.

This manual, which is supplemented monthly, is a two-volume source document for obtaining data on any protection problem. Information contained in the manual covers the broad range of subject areas required to protect the modern enterprise from nonbusiness losses.

69. Ward, C. Vandalism. London, England: Architectural Press, 1973.

A collection of articles examining vandalism, with emphasis on related psychological, sociological, economic, and architectural considerations, drawing upon British and American experience. Initially, an attempt is made to go beyond the concept of vandalism as meaningless violence. Vandalism is shown to have both expressive and instrumental value. It can be a form of social protest, a reaction to environmental stimuli, or even an attempt to assert one's masculinity. Professional responsibilities of the architectural designer are examined. The authors show how design considerations can minimize the impetus and opportunities for vandalism, as well as its consequences. Legitimized vandalism is seen in the examples set by motorists, industry, government, and others who noncriminally damage the environment. Finally, solutions are proposed, such as deflection of the behavior to other less harmful, or constructive, alternatives. Legislation, community action, and education, improved protection and detection methods, and punitive deterrence methods also are explored.

70. Weber, T. L. Alarm Systems and Theft Prevention -- An Expert Says: "Think Like a Thief." Los Angeles, CA: Security World Publishing, 1973.

Discusses top-security alarm systems, the methods by which they are being defeated, and the countermeasures currently available against such methods. Explains the economics of alarm system choice, as well as the problems of police-connected alarms, the types of safes that can prevent successful attacks, and the pros and cons of the proprietary alarm located on the premises.

71. Wright, K. G. Cost-Effective Security. New York, NY: McGraw Hill, 1973.

Presents a general introduction to securing all types and sizes of business against internal pilferage and crimes against property perpetrated by outsiders. Addressed to business managers, it discusses in layman's terms many issues pertaining to security.

72. Westinghouse Electric Corporation. Justice Institute. Cargo Security Survey of the Port of Hampton Roads. Prepared for the U.S. Department of Justice, Law Enforcement Assistance Administration. Arlington, VA: Westinghouse Electric Corporation, November 1973.

Presents the findings and recommendations of a cargo security survey of five waterfront installations for improved security as may be realistically implemented with minimum increased cost. Among others, the recommendations provided cover: Perimeter security, lighting, parking, access control, receiving and distributing cargo, and treatment of high-value cargo.

73. _____. Justice Institute. Port Security Study for Wilmington, Delaware. Prepared for the U.S. Department of Justice, Law Enforcement Assistance Administration. Arlington, VA: Westinghouse Electric Corporation, January 1973.

Assesses the security of the Port of Wilmington and provides recommendations for improvement in the areas of Port police, physical security (fencing and lighting, cargo cribs, warehouse security, key control, planned construction), vehicle movement control, and cargo documentation control.

CONTINUED

2 OF 3

INDIVIDUAL AUTHOR INDEX

Individual Author Index (Continued)

Individual Author Index (Continued)

TITLE INDEX

Title Index (Continued)

Title Index (Continued)

Title Index (Continued)

SUBJECT INDEX

Subject Index (Continued)

NOTE: Most bibliographic entries indexed to broad categories (e.g., Planning/Design) also discuss more specific design concepts (e.g., Access Control) and may not herein have been crossindexed as such.

END