Instructor
Text

Modular Explosives Training Program

Bomb Security Guidelines
The Preventive Response

Bureau of Alcohol,
Tobacco and Firearms

ATF P 7550.10 (3/76)
(replaces ATF T 5145-14)

To be used in conjunction with
modules 12 & 13 of Instructor Guide

BOMB SECURITY GUIDELINES

The Preventive Response 08

THOMPSON S. CROCKETT
GEORGE B. GOERING

CONTENTS

A PUBLICATION OF **The National Bomb Data Center**

Research Division □

A program funded by the Law Enforcement Assistance Administration of the United States Department of Justice. Dissemination of this document does not constitute U. S. Department of Justice endorsement or approval of content.

BOMB SECURITY GUIDELINES

The Protective Response

> "Listen closely . . . This is Weatherman . . . There is a bomb at 240 Centre Street . . . You have just enough time to get out if you leave now . . . Make sure everybody gets out . . . Do not try to find it . . . This is for real. We're dead serious."

This warning was received at 6:43 p.m. on June 9, 1970, at the New York City Police Headquarters Communications Center from an unidentified male.

At 6:45 p.m. the same evening, the following call was received in the Office of the Chief Inspector, New York City Police Department, again from an unknown male:

> "A bomb was placed in police headquarters and scheduled to go off . . . This is a warning so that the building can be evacuated so that no one will be hurt . . ."

At 6:57 p.m., 14 minutes after the first warning was received, a bomb exploded in a second floor men's room at Police Headquarters while a search was in progress. Three police officers and an elevator operator in the building were injured and four persons were injured by debris hurled into the street below.

This is an example of the violent increase in the use of the bomb across the United States as a weapon of intimidation, destruction, and death. Terroristic and criminal bombings have taken the lives of scores of persons, maimed and otherwise injured hundreds of others, and caused millions of dollars in property damage. With increasing frequency, private institutions and business firms are requesting aid from public safety organizations in evaluating existing security programs and developing new preventive measures. The purpose of this publication is to provide public safety personnel with background information and the basic procedures necessary to assist the public in making effective physical security plans and to aid the police in the protection of their own facilities against the rising attacks by explosive and incendiary devices.

The Alcohol, Tobacco and Firearms Division of the U. S. Treasury Department conducted a special survey of the bombing incidents which occurred from January, 1969, to June, 1970. During that period, 4,330 bombings were recorded and of that total, 3,355 were classified as incendiary and 975 were explosive. This indicates that during the interval covered by the survey, the use of incendiary devices, such as Molotov cocktails, was three times as great as explosive devices. However, the chronological, monthly Summary Reports on bombing incidents, initiated in July, 1970, by the National Bomb Data Center, report that from July 1, 1970, to April 30, 1971, 1,227 bombing incidents occurred: 603 incendiary and 624 explosive. There seems to be a definite increase in the use of explosive devices in bombing incidents in proportion to those of an incendiary nature. While this discrepancy may be partially attributed to the two different methods of data gathering employed by the studies, the implications are too great to ignore.

Incendiary devices are not generally considered to be as dangerous a threat as explosives. When an incendiary bomb ignites, there may be time to evacuate the area in an orderly manner and, perhaps, even sufficient time for the building occupants to extinguish the blaze before the arrival of the fire department. In contrast, when an explosion occurs the detrimental effects are, for all practical purposes, instantaneous.

A bomb threat, itself, is an effective means of disrupting business and education, curtailing production, and diverting public safety personnel from other essential duties. From January, 1969, to June, 1970, the Treasury Department reported that there were 35,000 bomb threats, an average of 150 per day, in addition to the actual and attempted bombings. The evacuation of occupants from schools, businesses, and public buildings results in a significant loss of work time. The General Services Administration estimates that 130 evacuations of federal government personnel upon receipt of bomb threats during the surveyed period resulted in a loss of 2.2 million dollars in man-hours.

Since the bombs used in the recent wave of terrorist activity in the United States have ranged in size and shape from the flip-top cigarette package (containing an effective incendiary device with a wristwatch timing mechanism) to a truckload of oil-soaked commercial fertilizer, which caused $500,000 damage when exploded by terrorists, no organization should feel secure against a bomb attack. Unfortunately, there is no guide or device which can enable security personnel to positively identify every incendiary or explosive bomb. Consequently, any area which management fails to protect may become the objective of an activated bomb.

Although there is no security formula which can render every target immune from attack, a good security plan, properly executed, will reduce the threat of a successful bomb attack and the resultant destruction of property, personnel casualties, and disruption of operations.

The assignment to develop and administer a security plan for preventing bomb attacks is a challenging one. Three successful criminal bombings in Manhattan in 1970 have demonstrated that some bombers are well-organized, skillful in the use of explosives, bold, resourceful, and willing to devote the time and effort necessary to select, survey, and penetrate their targets. They were able to shatter three corporate offices within minutes. Obviously, the public or private security officer is faced with a potentially formidable adversary.

An earlier publication, *Bomb Scene Procedures,* was devoted to the development and execution of the bomb incident plan, which includes the recommended action to be taken upon receipt of a bomb threat or the finding or detonation of an explosive or incendiary device. This publication will cover those procedures which can be employed to reduce the risk of bomb attack, a process often referred to as *hardening the target.* These procedures are also referred to as physical security measures, defined by the United States Army as:

> Steps taken for the protection of property, personnel, material, facilities, and installations against unauthorized entry, trespass, damage, sabotage, or other illegal or criminal acts.

Thus, physical security deals with prevention and is designed to protect against not only bombing incidents, but a full range of possible attacks.

The recommendations, both general and specific, that are made in the following sections are intended as guidelines to intelligent action based upon a comprehensive review of each specific situation. Each point discussed is obviously not applicable to every facility and it is even possible that an extraordinary situation may arise in which none is applicable. In such a case, expert advice must be sought. Techniques and priorities of action will, of course, vary with the availability of funds, the local estimation of risk, manpower, time, and other factors.

SECTION ONE
SECURITY PLANNING

The planning of security measures for the prevention of bombing attacks should be based upon five basic concepts or principles.

1. **An accurate assessment of the vulnerability of the installation and the risk of attack must be made.** Vulnerability is generally determined by a security survey and risk is estimated on the basis of current intelligence.

2. **Security must be based on relative rather than absolute protection.** Since the cost of security normally increases in proportion to the protection provided and since absolute protection against bombing attack is virtually unachievable for most installations, protective measures always represent a compromise of values.

3. **Responsibility for the development and implementation of security measures rests with those officials responsible for the management of a facility.** Whether public or private, management should plan and execute defensive measures against a bombing attack. This responsibility cannot be delegated or avoided by those in authority.

4. **Security measures should make maximum use of the existing operating structure, proven supervisory and technical skills, and materials and equipment on hand.** The use of available resources not only reduces security costs, but also emphasizes the fact that effective security must involve all endangered personnel.

5. **Operational readiness is essential to security.** Once security plans have been developed, they must be constantly reviewed, tested, and revised if they are to retain their effectiveness.

THE SECURITY PLANNING CYCLE

It has often and accurately been stated that planning is a continuous process. In this context security planning should be regarded as a cyclical procedure. Figure 1 illustrates six sequential steps or phases that must be repeated periodically, if not continuously, in order to assure an effective security preparedness. This, of course, is true whether planning for security against all forms of attack or in specific response to the threat of bombing. In fact, the distinction is largely irrelevant since the measures involved in bomb security are no different than those aimed at the prevention of other forms of sabotage.

The six planning steps listed below are discussed in some detail later in this section.

Assessment of the Situation. An effort should be made to assess the risk of attack through an intelligence study and to determine the vulnerability of the facility through a security survey.

Security Policy. Since total security is impossible and protection is expensive in terms of manpower and resources, management officials must determine what levels of security will be established for various portions of the facility.

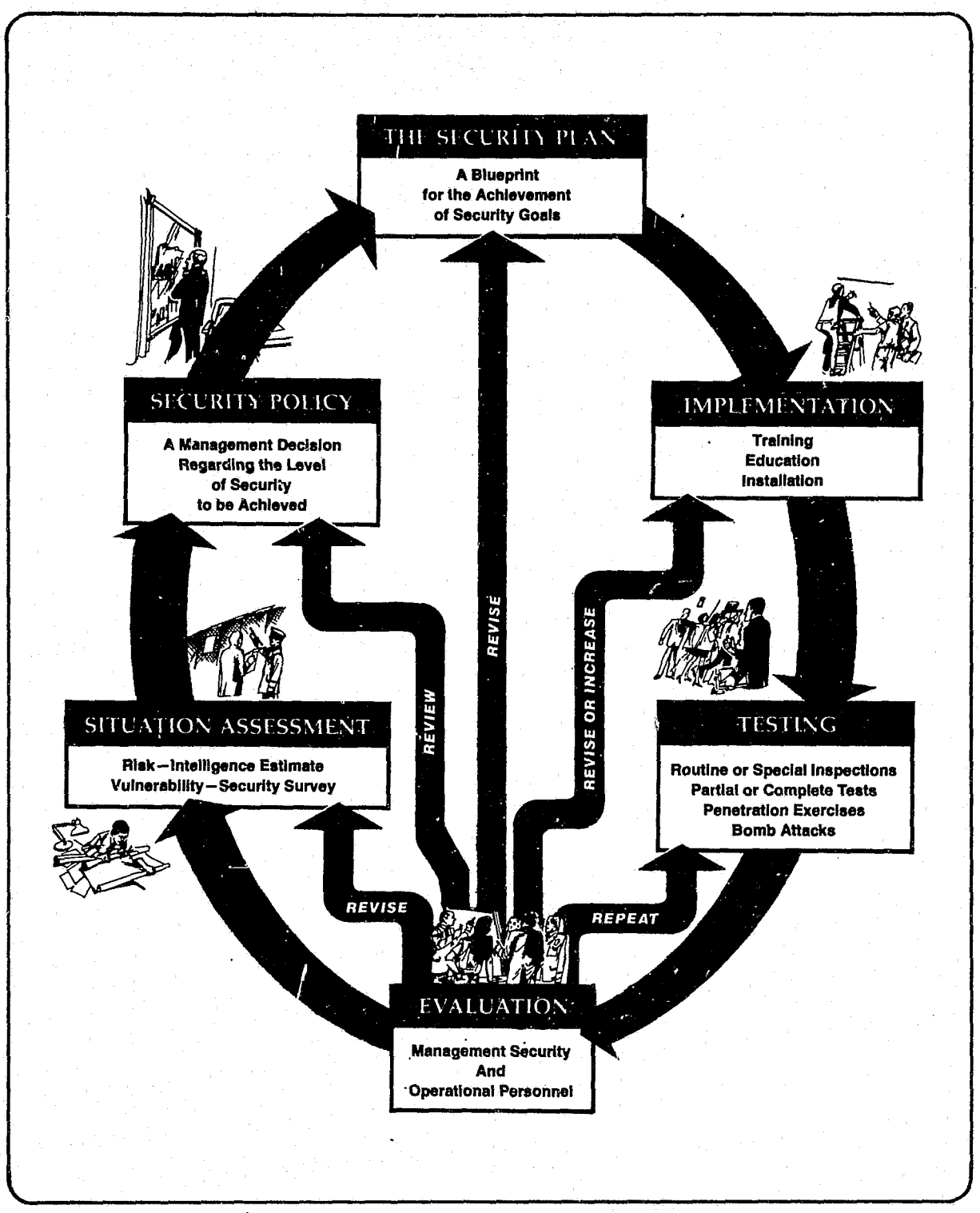

Figure 1
THE SECURITY PLANNING CYCLE

- *The Security Plan.* A blueprint or plan for the achievement of security goals must be developed and published.

- *Implementation.* The security plan must be implemented, including necessary training and education of personnel and installation of required systems and protective devices.

- *Testing and Inspection.* Partial and complete tests of the security plan must be conducted and a continuing inspection system activated.

- *Evaluation.* Management, security, and operational personnel must all be involved in the evaluation of the security plan based on routine operations, scheduled tests, and actual bomb incident experience.

THE SECURITY OFFICER

It is difficult to imagine how adequate security planning can be accomplished without the leadership of a security officer. Whether security planning and execution is a full-time assignment or a supplementary duty in the organization, the security officer should be carefully chosen on the basis of background, experience, and interest.

In large or decentralized organizations or facilities, it will be necessary to appoint security officers or assistant security officers for each location since the security officer must be familiar with the personnel and structures that fall within his area of responsibility. In police or fire organizations, for example, a security officer would be appointed for the headquarters complex and additional officers or assistants named for each precinct station or firehouse. Organization for command purposes will generally follow the existing pattern of the organization for decentralized personnel. For police agencies in those areas where the risk of attack is clearly identified, a *full-time* security officer should be considered, with security assigned as an additional responsibility for selected personnel in district or precinct facilities.

The security officer, subject to supervision by the management of an organization, should be charged with the responsibility for the overall development and administration of security plans. He should also be responsible for the design and implementation of appropriate response actions to deal with attacks where preventive measures have failed.

The first and most important step in security planning is an accurate assessment of facility vulnerability and risk. As previously noted, the security officer will generally base his risk assessment on current intelligence, and his vulnerability evaluation on a comprehensive physical security survey. Both sources of information provide essential data upon which security recommendations can be made to management. Without a continuing, systematic, and effective assessment program, security costs will pyramid exorbitantly or protection will diminish to the point of ineffectiveness.

SITUATION ASSESSMENT

Risk: Intelligence Collection

Security assessment and planning requires the continuous collection and evaluation of information about recent attack incidents in the United States. In the case of bombings, the

processing and evaluation of this information will result in intelligence which performs at least three essential functions:

1. To insure that security plans for bomb attack prevention and actual incidents are appropriate and practical for the area to be protected.

2. To serve as a basis upon which to select a security posture or plan which will be proportionate to the existing or potential threat.

3. To provide for updating or revising plans to include countermeasures against new techniques encountered in actual bombing activities.

The type of information to be collected in the intelligence gathering process should answer as many of the following questions as possible.

- Has the organization or facility been the target of a bomb attack or the recipient of a bomb threat?

- Have similar organizations in the country been the targets of bomb attacks or the recipients of threats?

- In recent bombings, attempted bombings, or bomb threats:

  What was the target?

  Where was the explosive or incendiary device placed?

  How was the bomb delivered?

  How did the bomber gain access to the target?

  What incendiary or explosive device was used? Did it include a timing mechanism or other delay fuze?

- If a warning message or telephone call was received:

  Did it specify where the bomb was located and/or when it would detonate?

  To whom was the message addressed and how was it received?

  Who or what office received the threatening telephone call?

- What was the day and time of the incident? Is there a pattern?

- What security measures in effect at the time were compromised, neutralized, or circumvented? How was this accomplished?

- What security measures might have prevented the attack?

- Did the news media or informers report any recent threats of bombings by any group which is active in the area, or against the kind of target protected by the security officer?
- Are terrorists or suspected terrorists either present or en route to the community?
- Has the theft of explosive materials, or materials which can be used in the manufacture of explosives, occurred in the community?
- What levels of bomb technology and tactical doctrine are available to groups that employ or may resort to bombing attacks?

In order to be adequately prepared to meet an attack threat at any given time, background information on bombing trends can best be obtained in the local area from law enforcement intelligence units, the news media, established sources of information, and neighboring communities and allied agencies. National trends can be obtained from the National Bomb Data Center operated by the International Association of Chiefs of Police. Monthly NBDC Summary Reports provide public safety officials with a chronological description and statistical analysis of bombing incidents. Statistical tables include:

- Incidents by population group.
- Incidents by region of the country.
- Number of bombs by population group and region of the country.
- Motive or intent of bombers.
- Target.
- Type of bomb or incendiary device.

In addition to its monthly reports, the National Bomb Data Center will prepare special statistical analyses in response to specific requests from public safety officials.

Information relating to the theft and recovery of explosives will eventually be available from the Alcohol, Tobacco and Firearms Division of the U. S. Treasury Department. Inquiries should be directed to regional ATF offices.

Vulnerability: The Security Survey

When intelligence indicates a risk of bomb attack, a comprehensive physical security survey should be conducted to identify security hazards and deficiencies and to develop recommendations for minimizing or eliminating the opportunity for an attack.

A written report of the physical security survey is essential to enable reviewing officials to determine the scope and adequacy of the survey; to substantiate the need for additional security studies of certain areas, if deemed appropriate; and to provide a basis for decision making regarding the adequacy of the existing security system or the need for additional measures. The report must be handled and stored in a manner that will protect it from all unauthorized persons since it will

identify critical areas, security hazards, existing security precautions, and recommendations for additional security measures. Its disclosure to unauthorized personnel could result in a successful bombing of the facility.

While the exact written format of the physical survey report is not important, the report should include at least the following information:

- Identification of building, area, or structure surveyed.
- Date of survey.
- Name of survey official.
- Address or location of object of survey.
- Pertinent history – including a brief statement of operations, number of personnel, and record of previous bomb incidents, if any.
- Structure – including physical characteristics and a general description of the building or structure, setting, and surrounding area.
- Identification and location of critical areas.
- Identification of critical functional elements, whose destruction or damage would totally halt productivity.
- Security measures presently in effect.
- Security devices installed which are not in use, or in need of repair.
- Security weaknesses.
- Recommendations.

The physical security survey should be made by *only* individuals experienced in the conduct of physical security measures, to insure that any recommendations made are appropriate, practical, and cost-effective. The survey assignment is usually given to the security officer when one has been appointed. If the organization does not have a security officer, a project manager may be designated to administer a physical security survey conducted by a professional security consultant, on a contract basis.

Once the decision has been made to conduct a physical security survey and the task has been assigned to a security officer, six preliminary steps are recommended. These early preliminaries are especially important if the security officer is an outside specialist working under contract or an employee, who has experience in conducting a survey, but has little or no background information on the facility to be surveyed.

- Schedule a meeting with management officials to arrange for necessary assistance and coordination during the survey.
- Obtain a working knowledge of the 'round-the-clock operation of the facility.

- Obtain floor and ground plans of the area whenever possible.
- Obtain and review details of previous bomb incidents at the facility to be surveyed.
- Obtain and review details of bomb incidents at similar facilities throughout the nation.
- Obtain and review details of bomb incidents which have occurred in the surrounding communities.

Survey Parameters. Throughout the conduct of the physical security survey six questions should be considered:

- What is the area to be protected?
- Where could a bomb be concealed inside or adjacent to a target?
- How could an incendiary or explosive device be successfully employed against the target?
- What measures can be employed to prevent an attack against the target?
- What measures can be taken to minimize damage in the event that a device detonates or ignites in the target area?
- What are the costs of these security measures?

Target Analysis. During the survey, the entire production process of the facility must be analyzed to determine the key functional elements which are vital for the operation of the system and hence may be the target of a bomb attack. These critical factors are often overlooked, misidentified, or oversimplified due to their often ordinary or commonplace nature. For example, in a security survey made of a steel rolling mill, the individual rolling machines were initially considered to be the elements requiring high priority protection. Further study revealed that all of the rolling machines were electronically controlled by computers. However, if one, two or even ten of the computers were damaged by carefully constructed and strategically placed bombs, the total output of the plant would only be decreased, not completely halted. But if, in addition, the main electrical power lines serving all the equipment within the plant were knocked out, production would be completely stopped. The delay could conceivably last for a one to three day period while repairs were made, unless the facility had access to emergency power generating equipment.

A detailed, systematic study of each separate function within a facility and its relationship to all other operations will eventually reveal the "common denominator" in the majority of these procedures. In the case of the steel mill, the "common denominator" or the single most vital element employed throughout the plant turned out to be water. Water was constantly used in all phases of production, and the removal and replacement of the damaged water pump would take several weeks or longer, during which the entire plant would remain inoperable.

A properly performed security survey will determine which areas require high priority protective measures and emphasize additional vulnerable points such as railroad switch boxes, fuel storage areas, vehicle parking areas, and specific office spaces. The positive identification of potential

primary targets will enable a facility to effectively allocate their available funds to achieve maximum protection.

As the level of security is increased, the cost increases, making it important for the survey officer to endeavor to recommend only those physical security measures which can most effectively and economically provide protection commensurate with the threat. In some instances costs will hinder an organization from protecting the entire installation. It then becomes necessary to determine the relative vulnerability and critical importance of various areas, so that security resources can be used to optimum advantage.

The detailed security survey must attempt to obtain all pertinent data. A thorough, systematic procedure should be followed, similar to that employed in a crime scene search, which will insure that all physical security hazards or deficiencies are noted. On-site inspections should be conducted during periods of peak activity, as well as during hours of daylight and darkness, even though the area being surveyed is not in operation at the time. The work flow and production movement patterns must be surveyed to identify those areas which are vulnerable to penetration and attack.

SECURITY POLICY

The physical security measures for an organization or facility should be no more extensive than warranted by a careful consideration of the situation. Based on an estimate of risk provided by the intelligence survey and the existing levels of security as revealed by the security survey, management officials must consider such factors as the effect of security measures on morale, the impact of security measures on productivity, the availability of funds, the potential damage or loss from bombing, the existing resources available for security programs, as well as the legal obligations, in determining what level of security will be provided for their facility.

Considering the cost-effectiveness characteristics of physical security, it is quite likely that management will conclude that a multi-level security program is most feasible. Such a program involves a rating of functional areas based upon their importance to productivity and the value of their contents. The concept of critical area identification was developed by the Industrial Security Branch of the Office of the Provost Marshal General, Department of the Army, and recently was reprinted in *A Checklist for Plant Security* issued by the National Association of Manufacturers.

Identification of critical areas. The protection of plant and equipment in emergencies is basically a matter of compromise. As the degree of protection rises, so does the cost. The problem of what and how to protect becomes a question of weighing the importance of the plant and equipment against the returns that can be expected from the protection provided.

Maximum effort should be expended in protecting areas that are critical to the plant operations. Short supply and long lead-time equipment should be given next priority for protection. Delicate instruments, for example, would require greater protection than large cranes. Items of machinery or equipment that have the capability of self-destruction, or of causing serious damage to other machinery or equipment, would require a high priority.

The basic unit of planning to minimize damage, and provide for rapid resumption of operations is the *functional area.* A functional area is composed of a group of machines or equipment performing related functions or operations. However, since all areas are not of equal importance, it is neither economically feasible nor theoretically necessary that they be afforded equal consideration in planning for protection and restoration of production or service. Management, as the first step, must determine which functional areas warrant primary consideration.

The functional areas warranting primary protection may be identified by analyzing two factors:

(1) The relative importance to overall production or operation.

(2) The relative vulnerability of machines and equipment to damage.

At the top of the scale would be a plant area which is highly important to overall production and susceptible

to damage. These functional areas nearest the top of the scale should receive top priority.

The relative importance of each functional area can be determined by conducting a *Functional Area Criticality Study.* The first step in this study is to group all of the functional areas into two or more general categories. The following categories are suggested:

Group A—Those whose loss would cause an *immediate stoppage* of production or operation because production equipment or parts would be lost.

Group B—Those whose loss would *reduce* production or operation because of a loss of productive equipment or parts.

Group C—Those whose loss *would not have an immediate effect* on production or operation but would require additional manpower to maintain their function.

Group D—Those whose loss would have *no direct effect* on production or operations.

The functional areas within each group should be ranked according to their vulnerability to damage. As the character of production or operation changes, the grouping should be revised to keep the ranking current. Since the more important operations will be included in Group A, further detailed investigation can be confined to this category.

The relative importance of the functional areas placed in Group A is dependent upon the extent to which the following factors control the production or operation recovery time.

(1) Length of time to rehabilitate or procure machines, equipment, and raw materials (lead-time).

(2) Length of time for tier contracting, i.e., time for subcontract to be let and contractor to start volume production.

(3) Length of time to develop alternate operations.[1]

Unfortunately, the critical area identification concept suffers from a major deficiency. Since the concept was developed in the context of civil disorder situations, it is basically oriented toward the protection of property and production. When responding to the potential hazards of a bombing attack, plans must include protective measures that will cover the possibility of human injury or death. However, this concept can be easily extended to incorporate a consideration for human risk in determining the appropriate levels of protection in the security policy.

THE SECURITY PLAN

When an accurate assessment of the situation has been made through the analysis of intelligence and a comprehensive security survey, and when management has formulated a policy that sets overall security goals, a detailed security plan must be developed. The security plan should be a blueprint for the achievement of a relatively permanent state of being rather than a set of procedures to be implemented at some point in time in response to some specific incident or event. The plan should also describe how human and fiscal resources will be allocated to provide a predetermined level of continuing physical security against bombings and/or other kinds of attacks.

Scope and Format

Bomb security plans range in scope and format from the detailed and elaborate industrial defense plans against sabotage to relatively simple security plans developed to protect a single building specifically against bomb attack. While the magnitude of industrial defense planning may exceed the needs or abilities of smaller public and private facilities, the principles involved are essentially the same. The following outline shown in figure 2 of an industrial defense plan was adapted from a publication entitled *Industrial Defense Against Civil Disturbances and Sabotage,* which was released in 1969 by the Office of the Provost Marshal General, Department of the Army, Washington, D. C.

---

[1] *A Checklist for Plant Security,* National Association of Manufacturers, undated. Based on Department of the Army Industrial Emergency Planning Guide against Civil Disorders, released May 2, 1968.

INDUSTRIAL DEFENSE PLAN
AGAINST
CIVIL DISTURBANCES–SABOTAGE

INTRODUCTION TO THE PLAN. (This presents the foundation on which the plan is based)

1. PURPOSE. (This paragraph should include a statement or statements comparable in scope to the following: "To establish a continuing program of preparation for protection against civil disturbances and sabotage, and to insure the continuation or restoration of essential operations in the event of other hostile or destructive acts.")

2. ASSUMPTIONS. (Assumptions stating in substance the premises shown below should appear in this paragraph.)

a. National.

(1) Potential civil disturbances in the United States could, with little or no warning, seriously endanger selected areas within the U. S. industrial base.

(2) Widespread sabotage against U. S. industry is not inconceivable.

b. Local. Each facility is vulnerable and subject to sabotage, civil disturbances, and other hostile or destructive acts.

3. BASIC PLANNING DATA. (This paragraph should include information as listed below.)

a. Maps. (Attach as appendix a topographical map showing the facility and surrounding areas, including the road and rail nets, the locations of neighboring industrial facilities, power plants, pumping stations, etc. Indicate on the map the location of residence of key employees residing in each area. Indicate the distance most of the employees live from the plant, i.e., 11-25 miles or whether there is no general pattern.)

b. Vulnerability. (The degree of vulnerability to civil disturbances is contingent primarily upon sociological, environmental, and geographic factors. Vulnerability to sabotage may in addition to these factors include criticality of the plant, criticality of the product and accessibility to the plant.)

c. Physical layout. (Maps, blueprints, and schematic drawings of production and or assembly lines.)

d. Operational data.

(1) Personnel. (Indicate the total number of employees and specify the number of contractual or vendor personnel present daily.)

(2) Shift operation. (Indicate the total number of employees and contractual personnel, male and female, assigned to each shift.)

4. EMPLOYEE TRANSPORTATION. (Indicate the mode of transportation used by employees for getting to and from work, i.e., 60 percent bus, 30 percent private auto, 10 percent subway.)

Figure 2
SAMPLE INDUSTRIAL DEFENSE PLAN

5. TRAINING AND TESTS. (This paragraph should contain instructions for training and rehearsing personnel and testing the plan.)

6. IMPLEMENTING INSTRUCTIONS. (Include a statement to the effect—this plan is effective immediately for training purposes. It will be effective for emergency actions when ordered by (specify the job title(s) of the person(s) with authority to partially or completely implement the plan under emergency conditions.))

SIGNATURE
(Senior Executive)

ANNEXES

I	Emergency Organization	VI	Planning Coordination and Liaison
II	Personnel Protection	VII	Records Protection
III	Fire Prevention	VIII	Damage Reduction
IV	Plant Security	IX	Restoration
V	Utilities and Services	X	Emergency Requirements
		XI	Testing

ANNEX I EMERGENCY CONTROL ORGANIZATION

1. **Chain of Command**
   a. Legal aspects
   b. Succession list
2. **Personnel Utilization**
   a. Emergency assignment records
   b. Recall of retired personnel
3. **Medical Requirements**
4. **Welfare Services**
   a. Emergency services for employees
   b. Employee situation briefings
5. **Control Centers (Command post)**
   a. Location
   b. Equipment
   c. Operation
6. **Emergency Notification**
7. **Emergency Organization (See figure 3)**

ANNEX II PERSONNEL PROTECTION

1. **Evacuation**
   a. Buildings
      (1) Evacuate by departments if practicable
      (2) Exits
         (a) Primaries
         (b) Alternates
   b. Plant
      (1) Away from the emergency area
      (2) Toward evacuation routes if possible

c. Routes
   (1) Pre-select evacuation routes in coordination with local law enforcement officials
   (2) Emphasize the importance of following these routes
   (3) Inform employees, pre-emergency, of evacuation procedures

2. **Assembly Areas**
3. **Shelters**
   a. Requirements
   b. Operations

ANNEX III FIRE PREVENTION

1. **Existing Fire Defense System**
2. **Arson Investigation**
3. **Emergency and Back-up Fire Services**

ANNEX IV PLANT SECURITY

1. **Security Plan.** (Outline the emergency organization and responsibilities of the plant security force. The normal organization and responsibilities should be adapted to meet the requirements imposed by a civil disturbance, sabotage, bomb threat, unexploded ordnance or other hostile or destructive acts. The security plan should include all actions and techniques to be employed to protect personnel, materials, products or services, premises and process from hazards inherent in operations and other acts mentioned above. The security organization of a facility will depend almost entirely on the size, criticality and vulnerability of the facility.)
2. **Legal Rights and Restrictions.** (This is a most important element and must be understood by management and members of the security force. The facility legal counsel must coordinate with the city attorney, district attorney or other legal offices to determine the authority of the property owner, and his employees, in protecting property and life.)
3. **Liaison and Coordination.** (List the names (positions), telephone numbers, law enforcement agencies, (local, State and Federal) with whom the plan has been coordinated and liaison should be maintained.)
4. **Security Force.** (The organization of the security force should be tailored to meet the requirements of a specific facility. The security force is the most effective and important element of security planning. It is the only in-house element capable of physically responding, utilizing judgment in an incident.)
   a. Qualifications Standards
   b. Training
   c. Uniforms
   d. Weapons
   e. Organization
   f. Shift Changes
   g. Communications
   h. Limitations of Security Force Function
5. **Perimeter Barriers**
   a. Types of barriers
   b. Construction
   c. Posting

d. Protective lighting
e. Vehicle parking
f. Intrusion Detection Devices

6. **Control of Entry.** (Develop procedures for positive identification and control of employees, visitors, and vehicles. A positive means of identifying employees is the use of a photograph identification card. Samples of the identification media should be given to law enforcement officials. (This is essential for getting through police lines and during times of curfew.) Coordinate with the police the category of personnel essential to plant operations, i.e., engineer, maintenance, etc.)
7. **Protection of Critical Areas.** (Identify and list critical areas within the facility.)
8. **Arms Rooms.**
9. **Personnel Security.**
10. **Reporting of incidents.** (Show procedures as to how, when, where, and to whom incidents will be reported.)
11. **Bomb Threats.** (List address and telephone number of):
    a. Nearest military explosive ordnance disposal team
    b. Bomb disposal unit of local police force
    c. Local fire department

    (Show procedures to be followed upon receipt of bomb threat. This should be coordinated with local law enforcement officials, local fire department, and the nearest military explosive ordnance disposal (EOD) team.)
12. **Emergency Notification.** (Prepare an emergency notification list or chart of personnel to be notified in the event of civil disturbance, or other emergency. This list must be kept current.)
13. **Emergency Shutdown.** (Indicate procedures to be followed by security personnel during and after shutdown.)
14. **Safeguarding Classified Material.** (Specify procedures for safeguarding or removal of classified material. Security personnel should know how to contact custodians of classified material. They should also be advised of actions to be taken with regard to the Department of Defense Industrial Security Cognizant Office, if applicable.)

ANNEX V UTILITIES AND SERVICES

(The importance of utilities and services during an emergency cannot be overemphasized. The disruption of communications, electric power, water, transportation, or fuel sources could seriously impair or stop production. It is essential that these utilities and services be considered critical to the continuity of operations; that they be properly protected and adequate emergency back-ups be developed. Essential utilities and services to be considered are listed below. The details for each should be coordinated with the respective utility or service company.)

1. **Communications**
    a. Coordinate with local telephone companies
    b. Adequately cover plant area
    c. Back-up primary system with two-way radios, walkie-talkies, field telephones, or megaphones (bull horns).
    d. Monitor local and state police radios
    e. Monitor fire department radios
    f. Monitor hospital and ambulance radios
    g. Establish communications with adjacent plants and businesses
    h. Establish communications with management and key employees
    i. Train switchboard operators in emergency procedures

j. Inquire as to availability of telephone–radio mobile equipment–license and frequency are assigned to the common carrier
k. Designate male operators as alternates for females who may not report
l. Unlisted telephone numbers, at control center, for use by management and key executives. Don't have all telephone numbers plainly listed–a few determined harassing callers can keep your lines occupied.

2. **Electric Power**
   a. Coordinate this portion of the plan with local electric power companies.
   b. Emergency Power. (An auxiliary source for providing sufficient emergency power for lighting and other essentials. This should not be construed to mean a stand-by capability to continue full production operations. The following items are suggested:)
      - Generators
        - Show size and location
        - Fuel supply
        - Operators
      - Battery-powered equipment
        - Flashlights
        - Lanterns
        - Other battery powered sources of illumination

3. **Water**
   a. Secondary source for fire fighting, essential operational needs, drinking, and sanitation.
   b. Location of primary water main.
4. **Transportation**
   a. Primary routes of ingress and egress
   b. Alternate (emergency) routes
   c. Accessibility of alternate routes to suppliers
5. Fuel Sources, i.e., pipelines, coal, and diesel fuel. (Stockpiling for emergency use should be considered.)

ANNEX VI PLANNING COORDINATION AND LIAISON

(This is a most important element of the plan and is designed to assure mutual planning approaches and objectives. It also provides a means of keeping you abreast of the social climate and receiving advance warning of the imminence and possible magnitude of a disturbance. Coordination and liaison should be maintained with:)

1. **Facility Members and Locations.** (List the name and location of each industrial facility or organization of the mutual aid pact, or with which coordination has been affected. Indicate who in each facility or organization can approve the implementation of the pact during a civil disturbance. Also include any other mutual aid pacts with which you made unilateral agreements. Show restrictions, if any, on mutual aid assistance during riots or civil disturbances.)
2. **Local, State and Federal Officials.** (List the name, location, and telephone number of each agency with which coordination has been accomplished:)
   a. Law enforcement
   b. Fire departments
   c. Adjacent plants and business firms
   d. Employee union officials
   e. Local utilities
   f. Local news media for news release policy

3. **Communications and Control.** (List the primary and alternate methods of communications that will be used to alert the mutual aid pact members and local state and federal agencies and your facility. Include methods of alerting during normal working hours and non-working hours. Include the methods that will be used in controlling personnel at the scene of the emergency, including direction of police, fire, and emergency vehicles and crews. Coordination must be made in advance for use of facility security personnel, state, and county police, as applicable.)
4. **Facility Responsibilities.**
   a. Personnel. (List by job title the various skills that you have agreed to furnish the mutual aid organization. Maintain a current roster of these personnel by name, with alternates. Include supervisory responsibilities when aid is required.)
   b. Equipment. (List the material and equipment that your facility will have available for mutual aid. Establish a method of having the material and equipment delivered as needed.)
5. **Other Participants Responsibilities.**
   a. Personnel. (List by job title or skill, the personnel to be furnished by other mutual aid participants. Indicate procedure for their reporting, utilization, and control. Indicate responsibility for control and supervision for each group.)
   b. Equipment. (List the material and equipment that may be obtained from other mutual aid members. All items should be listed by location and include procedure for obtaining them.)
6. **Operational Procedures.** (List special limitations, legal aspects, feeding and transportation of personnel, prorating cost and use of any special items not covered above.)

Note.—The Mutual Aid Pact or Coordination Agreement may be substituted for part of this annex.

ANNEX VII RECORDS PROTECTION

1. **Classes of Records**
2. **Reproduction Methods and Priorities**
3. **Protection of Records**
4. **Protection of Computers**
5. **Operations**
6. **Cash, Negotiables, and Other Valuables**

ANNEX VIII DAMAGE REDUCTION

1. **Functional Areas.**
   a. Criticality. (List functional areas, in order of priority, most critical to overall facility operations. This should include consideration for all types of emergencies.)
   b. Protection. (Functional areas most critical to the overall operation and/or production should be given priority of protection, prior to, during and after the emergency.) Refer to plant security annex.
      (1) Buildings. (Include measures for reinforcing walls, roofs, floors and protection of wall openings such as windows and doors of existing buildings. These protection factors should be considered in new constructions.)
      (2) Machinery. (Factors to be considered are dispersal, protection of one piece of equipment by use of another, and parts removal.)
      (3) Hand tools. (Indicate individual action and responsibilities for protection of hand tools. Include tool crib dispersal.)
      (4) Special equipment. (Indicate methods used or to be used to disperse on- or off-site parts, sub-assemblies, completed items, jigs, dies, patterns, moulds, and other critical items.)

(5) Transportation. (Indicate dispersal location of transportation equipment to protect machine tools.)

(6) Utilities. (Indicate protection afforded utilities and include location and protection of electrical transformers at load centers and communications centers.) Refer to Plant Security Annex and Utilities Annex.

2. **Shutdown Procedures.** (Specify shutdown procedures to include methods and sequence for individual sections within the facility and the facility as a whole. Designate title (positions) of individuals responsible for implementing shutdown procedures.) Refer to Item 12, Plant Security annex.
3. **Fire Control.** (See Fire Prevention annex.)
4. **Dispersion.**(Consider the dispersion of machinery, material, and personnel.)
5. **Other Measures.** (List other measures peculiar to your facility that may be necessary to minimize damage.)

ANNEX IX RESTORATION

1. **Command Responsibilities and Control**
2. **Damage Assessment**
   a. Internal reporting
   b. External reporting
3. **Restoration Measures**
   a. Alternate sources of supply
   b. Stockpile
   c. Alternate production method
   d. Sub-contracting
   e. Utilities
   f. Salvage procedures
   g. Transportation

ANNEX X EMERGENCY REQUIREMENTS

(These requirements should be based on estimated needs for the duration of the emergency. These items should be pre-stocked because conditions may preclude their procurement during the emergency. Unused portions can be carried over for post-emergency use.)

ANNEX XI TESTING THE PLAN

(Frequent testing and correcting the plan will improve its effectiveness upon implementation under actual conditions. An emergency plan, like a chain, is no stronger than its weakest link.)

1. **Types of tests.** (Specify type of tests, whether partial or complete and when umpires or observers are to be present. Indicate frequency of partial or complete tests.)
   a. Partial—testing individual segments of the plan
   b. Complete—testing entire plan
2. **Tests should be unannounced**
3. **Weaknesses should be noted and the plan revised to include corrective actions.** (Include reports of test results by observers or umpires and action to be taken by designated company official to improve techniques and take corrective action on deficiencies.)

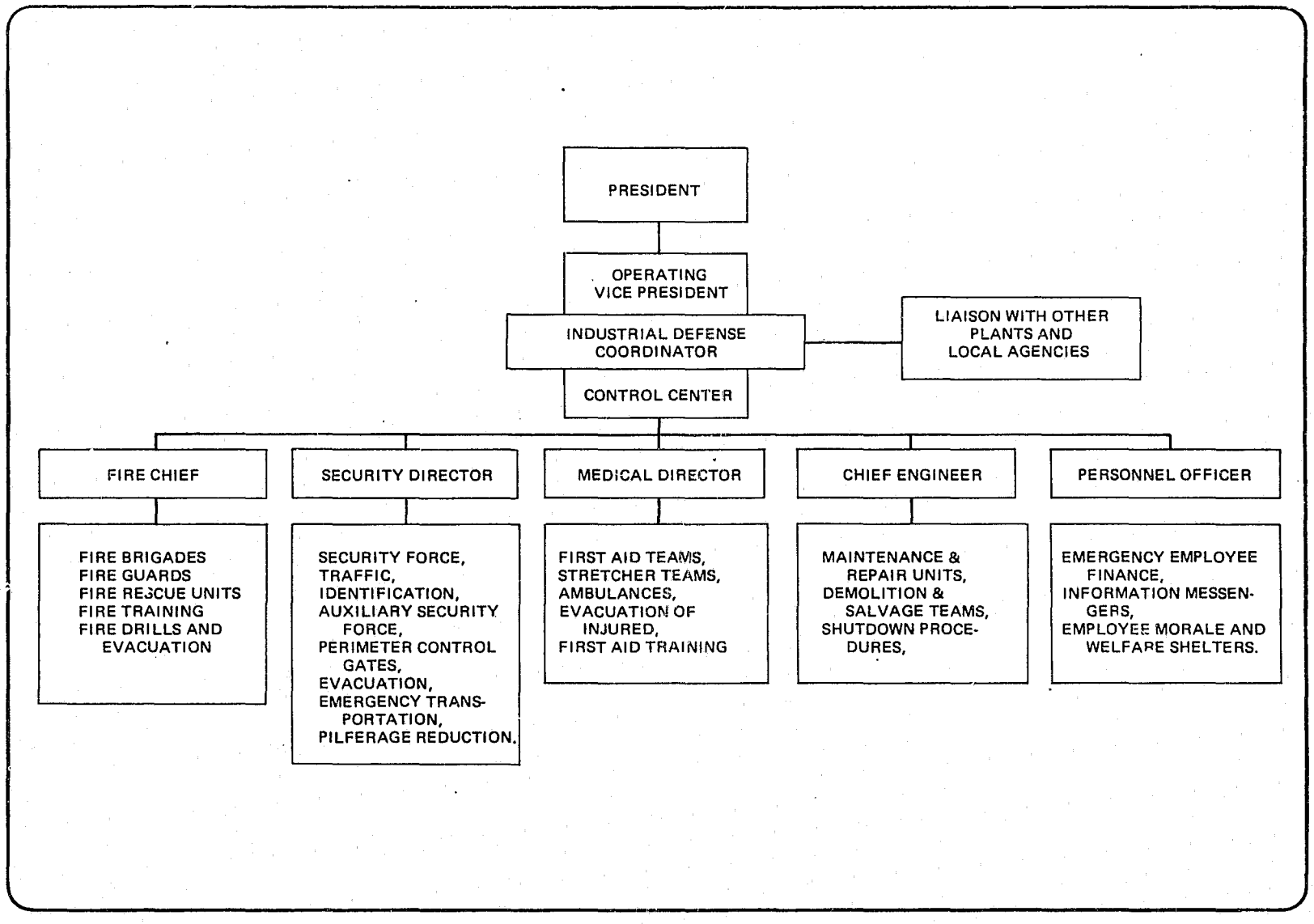

Figure 3
BASIC EMERGENCY ORGANIZATION FOR A LARGE INDUSTRIAL FACILITY

Figure 4 illustrates a simple bomb security plan developed to protect a high-rise county office building located in an urban setting. Since the plan is presently in effect, minor changes have been made to remove identifying data. Otherwise, it is presented as it was developed.

SECURITY PLAN FOR PREVENTING BOMB ATTACKS

1. **Background.** Terrorist bombings throughout the United States against structures which house federal, state, county, and municipal government offices have doubled during calendar year 1970. The incidence of terrorist bombings in increasing. A terrorist bombing of the County Building could result in serious damage which could impair the ability of this county to perform services vital to the community.
2. **Purpose.** It is the purpose of this plan to prescribe the procedures to be implemented for preventing a terrorist bomb attack against the County Building.
3. **Concept.**
   a. The concept upon which this plan is based is that of denying access to a terrorist bomber. Various security devices have been installed and security measures developed to prevent the criminal bombing of the County Building, to protect the occupants and contents, and to insure that the ability to perform vital operations is not destroyed if a bombing occurs.
   b. Security plans will be revised, when appropriate, and the security procedures in effect at a given time may vary, according to the circumstances.
   c. Security measures will result in personal inconveniences and in delays in normal operating procedures. The cooperation of each employee in supporting this plan is essential to its operation.
4. **Implementation.** The plan will be implemented upon order of the County Executive or his designated representative.
5. **Scope.** This plan is applicable to the property which is bounded on the west by Elm Street, on the east by Central Avenue, on the north by First Street and on the south by Second Street and to the building which is located thereon, i.e., the 10-story building in which the offices of the County Government and the various services of the county are located, and to all employees of the county.
6. **Critical Areas and Equipment.**
   a. These are areas and equipment which, if damaged by a bomb, could render the building uninhabitable, or could seriously impair the ability of one or more of the services of the County Government to perform functions vital to the welfare of the community.
   b. Critical areas are listed in Annex I.
7. **Special Security Provisions** are contained in Annex II.
8. **Command and Control** will be exercised by the Officer in Charge of the Emergency Operations Center.
9. **Procedures for Alert Condition 1** are set forth in Annex III.
10. **Procedures for Alert Condition 2** are contained in Annex IV.
11. **Procedures for Alert Condition 3** are prescribed in Annex V.

Figure 4
BOMB SECURITY PLAN FOR A COUNTY GOVERNMENT BUILDING

ANNEX I CRITICAL AREAS

The following areas are considered critical, with priorities for their protection indicated by the order in which they are listed:

1. **Transformer,** located in an underground vault in the building alcove, on the west.
2. **Transformer Switch Gear,** located in room 100.
3. **The Emergency Generator,** located in room 115.
4. **The Emergency Operations Center,** located in basement room 3, which houses the communications center of the Public Safety Division.
5. **The Radio Equipment Room,** located adjacent to the Emergency Operations Center.
6. **The Telephone Equipment Room,** located adjacent to the Emergency Operations Center.

ANNEX II SPECIAL SECURITY PROVISIONS

The following additional security has been provided for the County Building.

1. **Transformer Vault.** A chain-link fence and gate, with appropriate lock, has been installed at the alcove entrance; the entrances to the vault have been secured; electronic intrusion detection devices have been installed; access is controlled by the Emergency Operations Center.
2. **Stairwell Cages.** Cages have been installed in the stairwells at the ground level landings. These will prevent unauthorized entry into the basement, but will provide access to the stairwell by persons in the basement area. The cage doors are protected by electronic intrusion devices.
3. **Closed Circuit Television.** Closed circuit television systems, with moving image sensors, have been installed to monitor the elevator lobby at the entrance to the EOC.
4. **Package Holding Areas.** Blast-resistant package holding areas have been installed: one at ground level; one on the first floor, adjacent to an entranceway.
5. **Security Door.** An additional door has been installed at the end of the hallway which leads to the telephone equipment room and radio room. The door provides a means of emergency exit from the adjacent area and it must not be blocked. It may be opened only by means of a panic bar on the opposite side. Its use for other than emergency purposes is prohibited.
6. **Elevators.** Lockout switches for the elevator cars and floors and a car indicator panel have been installed in the EOC. Use of the elevator to gain access to the basement during security hours must be prearranged with the EOC.
7. **Entrances and Fire Exits.** All locks have been inspected, repaired or replaced, as necessary. Remote entrances have been alarmed.
8. **Security Hours Entrance.**
   a. During the hours that the County Offices are closed, access to the building is limited to the ground level south entrance.
   b. If directed, only the ground level south entrance and first floor east entrance will be used for entrance to, or exit from the building.
9. **Concertina.** Standard concertina barbed wire has been prestocked to provide for the emergency use as a temporary expedient to provide a barrier, when needed.
10. **Bomb Blankets.** The EOC is stocked with bomb blankets.
11. **EOC Guard.** Provision has been made for a guard post in the lobby, outside the EOC. Telephone lines have been installed.

12. **Badge system.** All employees have been issued photo badges.
13. **Security Lighting.** Around the building, security lighting has been installed to provide a uniform level of illumination.
14. **Locked Restrooms.** Doors to restrooms in the basement have had the markings removed and locks have been installed. Keys have been provided to adjacent offices. Public use is prohibited.
15. **Stairwell Doors.** Stairwell doors have been fitted with locks which can be locked to prevent access from the stairwell to floors other than those which are on ground level. Access into the stairwell will not be denied on any floor which is not on ground level.

ANNEX III ALERT CONDITION 1

1. **Instruct all employees to:**
   a. Be alert for suspicious activity.
   b. Look for objects which are conspicuously out of place, or strange to the area.
   c. Insure that visitors do not leave packages, or other objects in the building.
   d. REPORT AND LEAVE UNTOUCHED ANY OBJECT FOREIGN TO THE AREA.
   e. Report to EOC the arrival of outside maintenance or service personnel.
   f. Deny admittance of outside maintenance or service personnel to the transformer vault, EOC, or other critical areas until their identity has been verified and the purpose of visit authenticated.
   g. Observe and record the distinguishing characteristics or suspicious persons and vehicles.
   h. Omit from discussions with family and friends, the security aspects of their work or of the County Building.
   i. Report immediately to the EOC any unusual or suspicious incidents or persons.
2. **Search Teams.** Organize search teams for each shift.
3. **Tests.** Require daily testing of all electronic intrusion detection devices; record results; obtain necessary repairs.
4. **Exterior Lighting.** Provide for lamp replacement when they have been in use 80% of their rated life; inspect security of controls at least once each week; keep them clean and in good repair; turn on throughout hours of darkness.
5. **Building Exterior Patrol.** At least once each hour, on a random basis, inspect for evidence of tampering, verify security of tampering; verify security of transformer vault area; be alert for items which "do not belong" in the area. DO NOT TOUCH, BUT REPORT. Report burned out lights and be alert for persons loitering in the vicinity.
6. **Building Interior Patrol.** A continuous patrol of public areas should be maintained. Insure that doors to closets, mop rooms, etc, are closed and locked. Check stairwell cage doors and locks for evidence of tampering; question suspicious persons. Insure that fire exits are not obstructed.
7. **Emergency Equipment.** Periodically test, and verify the presence and serviceability of emergency communications equipment, electrical powers, lighting and fire equipment, e.g., extinguishers, standpipes, and first aid supplies.
8. **Maintenance.** Maintain good housekeeping by preventing the accumulation of trash in or around the building.
9. **Badge Control.** During other than normal hours of operation, sign-in, sign-out will be required of all persons and county identification badges must be presented by county employees. Persons who

forget or lose their badge must be vouched for by another employee in the presence of the guard. Visitors will not be admitted during these hours. Service and maintenance personnel who are not county employees must present identification, e.g., valid motor vehicle operator's license, the purpose of their visit must be verified, and an escort provided.

10. **Elevators.** Lock all elevators off in the EOC 30 minutes after the close of business. Turn all elevators on 45 minutes before the building opens for business. Persons who require the use of elevators at other times should call 267-4532.

ANNEX IV ALERT CONDITION 2

In addition to the preventive measures prescribed for Alert Condition 1, the following measures will be implemented upon order of the County Executive or his designated representative:

1. During normal hours of operation, all entrances will be secured, except one entrance at ground level south, and one east entrance on the first floor. Employees will be admitted upon presentation of their photo badge. Packages may be examined upon discretion of the officer on duty. Visitors will be screened on a random basis by a person who is knowledgeable of the County Building environment to determine the validity of their visit.
2. Access to the EOC will be limited to persons whose names appear on an access list maintained in the EOC. Official visitors and maintenance and service personnel must be escorted at all times while working in the EOC area.
3. Vehicle access to the building will be prevented by the installation of sections of concrete curbing across the entrance to driveways. These will be protected with barricades equipped with warning lights. A movable barricade will be installed at the entrance of the service road. Service vehicles will be admitted only after the purpose of their trip is verified.
4. The shipping and loading dock area will be guarded when the entrance is open.
5. Personnel access doors in the top of elevators will be secured with a county seal.
6. Stairwell doors will be locked to prevent access to floors above the first and ground level from the stairwell; install signs on lobby side of doors "Stairs to ground floor only—other levels locked."
7. During other than normal business hours:
   a. Two guards will be on duty at ground level.
   b. Exterior patrols of the building will be conducted at least two times each hour, using different routes, and on a random schedule.
8. Guard personnel will be immediately available to the EOC to respond to reports of suspicious activity in or about the building.

ANNEX V ALERT CONDITION 3

The following measures will be implemented, in addition to those prescribed for Alert Condition 1 and 2, upon order of the County Executive or his designated representative.

1. All persons will be screened to verify their purpose for entering the building.
2. All packages which might conceal a bomb will be searched or checked in the holding areas at the ground and first floor entrances.
3. The administrators of the services which occupy each floor are responsible for:
   a. Furnishing inspection services of the restrooms and adjacent stairwell landings for suspicious persons and objects once each 30 minutes during normal business hours.
   b. Providing for monitoring the activities of persons, other than employees, who enter their areas in order to detect suspicious activity.
   c. Denying unauthorized persons access to office areas where they will be out of observation at any time.
   d. The prompt reporting to the EOC of any suspicious activity or object.

Implementation

The security plan should be implemented only after management, security, and planning personnel are satisfied that it represents an adequate program for the achievement of organizational security goals.

Implementation of the security plan entails the training and/or education of the personnel involved and the installation of required security systems and devices. However, there is a tendency during the implementation stage to concentrate on the setting up of security equipment and the training of security guards and to exclude a thorough informative program for all facility workers and building occupants. This frequent mistake can cause unnecessary confusion and unfavorable reactions by uninformed employees.

Therefore, whenever security measures are placed in effect, they should be preceded by a security education program to acquaint all personnel with the nature and purpose of the planned restrictions. This program should endeavor to obtain the cooperation of all employees in complying with security regulations, in reporting suspicious activity, and in performing emergency duties when the occasion arises. Experience has proven that, to be successful, security education programs must be supported by top management. Any indication of command or supervisory indifference to the security plan will be quickly recognized by operational personnel and interpreted as an indication that the plan is unimportant. Employee cooperation is especially critical in the case of bomb security since the reporting of suspicious objects can lead to protective action that may save both lives and property.

Testing and Inspection

Once the security plan has been implemented, provisions must be made to insure that it is, and continues to be, effective. This is usually accomplished by a program of testing and inspection. Security inspections can easily be incorporated into existing command and supervisory inspection systems. Security personnel should conduct scheduled and unscheduled security inspections of all aspects of the implemented plan. For example, in police organizations, shift or precinct commanders should conduct security inspections of their areas of responsibility as part of their routine duties, while specially appointed security officers conduct periodic detailed inspections that resemble, in scope and nature, a security survey of a selected area. In all inspectional activities, the emphasis should be on identifying and correcting security weaknesses rather than simply determining the extent of personnel compliance with the existing security plan.

Security plans which, in addition to providing routine protective measures, call for increased levels of security under certain conditions, should be tested through the controlled implementation of those levels. Such tests can involve some or all levels of the plan, but they should be unannounced and timed to test the plan at its weakest point. A sudden tightening of security might, for example, be extremely difficult on a Sunday or at three o'clock in the morning.

Perhaps the second most effective test of a bomb security system is a penetration exercise. In this test an individual attemps to penetrate the security screen and place a simulated bomb inside the facility. Since this is normally done openly through access control rather than denial areas, there is little risk to the individual conducting the test. If the device is successfully planted and not reported

by security personnel or employees, it can also serve as the basis for an exercise of the bomb *incident* plan as detailed in *Bomb Scene Procedures.*[2]

Of course, the most reliable test of a bomb security system is the manner in which it functions during an actual bombing attempt. Incidents of this kind, whether successful or not, should be carefully studied for evidence of weaknesses in the system. In the case of equipment and even human components, a failure at another installation or facility can be studied for its implications to the local situation.

Evaluation

The last phase in the planning cycle is evaluation. Evaluation is a continuous process in the planning function. Management, security, and operational personnel should all participate in an almost constant review of data developed through actual bomb attacks, tests, and inspections, as well as through routine operations, to determine the need for positive action to improve the security system.

As indicated by the shaded arrows in figure 1, evaluation may result in:

- Additional testing and inspection.
- A review of organizational security policy.
- A revision of the security plan.
- Revision or increase in security education, training, or the installation of systems.
- Updated or revised intelligence collection.

[2]C. R. Newhouser, *Bomb Scene Procedures* (Washington, D. C.: International Association of Chiefs of Police, 1971). [An earlier publication of this series.]

SECTION TWO
INTRODUCTION TO SECURITY METHODS AND PROCEDURES

The certain security measures that can be taken to reduce the risk of a bombing attack are identified and discussed in this section. While established principles of industrial and military security serve as a basis for this discussion, their full coverage is beyond the scope of this publication.

SECURITY OBJECTIVES

Experience has indicated that for all property or institutional targets of bomb attack, there are four common security objectives which can minimize vulnerability and maximize protection.

- Denial of access to potential bombers.
- Use of existing and/or additional security measures and devices to protect critical or vulnerable areas.
- Identification and elimination, wherever practical, of areas where bombs could be concealed.
- Developments of a detection capability.

The common characteristic shared by all bombing attacks in the United States to date has been the need to deliver the bomb to the target area. For this reason, almost all protective measures are directed at access control. The principle followed throughout planning is that of *denying unauthorized access* and *controlling authorized access.*

In numerous federal and private buildings, access is limited to authorized persons, and items carried by these persons are subject to search, in an effort to prevent a bomb from being placed in the building. This is a practical and effective technique which is relatively easy to implement when a guard force and a pass or badge system are in use as part of the existing overall security program. However, there are also many buildings where security against bombing is a serious consideration, but where, for various reasons, it is not practical to control access to the building. Whether access to a building can be controlled or not, there are a number of security measures which can be used to raise the level of protection against a bomb attack.

While there are some obvious areas of overlapping, security measures that deal with denial of unauthorized access can, for the purpose of discussion, be classified as *denial procedures,* while security precautions aimed at controlling authorized access can be classed as *identification and movement control procedures.* Both denial and control procedures will be discussed following a more general review of target characteristics.

PRIME TARGET AREAS

In every facility there are two areas most likely to be selected for the placement of a bomb. In almost every facility the most vulnerable areas are those open to the public and the most critical areas are those housing essential utilities. In the current wave of symbolic bombings, devices have been placed primarily in public areas, but the determined bomber aiming for maximum property damage and disruption will most likely place his bomb in a utility area.

Public Areas

As previously mentioned, bombs have most often been detonated or ignited in areas accessible to the public. Public areas within a building usually include entrances, corridors, lobbies, stairwells, elevators, and restrooms. A building may also have other areas open to the public, such as retail stores, cafeterias, snackbars, newsstands, observation decks, bars, or garages.

Within the public areas of a building a bomb can be concealed in an enormous number of places, such as inside the cover of a radiator or window air-conditioner, beneath the surface of a draped display stand, in recessed fire extinguisher cabinets, in areas under stairways, atop or behind vending machines, or behind furnishings.

An assessment should be made of all locations in which a bomb might be concealed or placed unnoticed. In addition, notes should be made of the relative vulnerability of the various areas and recommendations should be made for limiting access or placing such areas under surveillance.

Public lockers provide an ideal place to conceal a bomb. If a building contains public lockers, consideration should be given to their removal, or the safety of their location evaluated. If their location is not relatively safe, it may be possible to have them relocated to an area where the risk of personal injury or property damage would be reduced in the event of a detonation. Or, protection may be added to areas adjacent to their present location. Master keys should be readily available for use in the event of a specific threat in which information is received that a bomb has been placed in a public locker.

Although not public areas, telephone equipment rooms and sink or mop closets are often accessible from public corridors because employees have made door latches inoperable by jamming a piece of paper in the latchway or taping the latch in its recess. This makes access more convenient for regular users, but it also provides another opportunity for the concealment of a bomb.

Trash storage or removal areas are a hazard in many buildings. These are often found in public or semi-public locations where building entrances may be unlocked or unguarded, even though security procedures for personnel access may be in effect at other building entrances. These unlocked and unattended entrances afford an excellent opportunity for both entrance and bomb concealment. Positive access controls for interior trash areas and the loading docks used for trash removal are essential for good security.

Trash is a peculiar problem, in that it can appear at irregular intervals and in unusual places. Nested, empty pasteboard cartons, packing materials from new office machines, or surplus or obsolete expendables abandoned during the course of an office move and placed outside an office in a public corridor, all give the bomber additional opportunity to conceal his bomb—or to deposit a burning cigarette. Trash should not be allowed to accumulate in mop rooms, remote stairlandings, storerooms, cafeteria and vending areas, or anywhere in the facility where the risk of explosion or fire is not acceptable.

Restrooms. Public restrooms have proved to be an extremely popular location for the concealment of bombs. In fact, in many facilities the restrooms are the first areas searched in the event of a bomb threat. Bombs have been found in unoccupied stalls which were locked from the inside. Also, they can be concealed in wastepaper or towel receptacles of any type. Security personnel should have a means of examining these containers, as well as a key for access to recessed receptacles. One method of checking disposal containers is to have them fitted with a plastic liner which the security guard can carefully lift in an effort to determine unusual weight which would indicate the presence of a suspicious object. The replacement of all waste receptacles and paper towel containers in public restrooms with an endless cotton towel dispenser or an electric hand dryer may also be considered.

Suspension ceilings with lightweight removable panels in public restrooms are a potential hazard. Some ceiling installations are low enough to enable a person to stand on a toilet seat, raise a ceiling panel, and place a bomb. In new construction or remodeling, consideration should be given to eliminating the use of removable ceiling panels in public restrooms and other public areas which are difficult to secure. In public areas which are considered highly vulnerable, a conventional plastered ceiling with a secured or sealed access panel will aid security.

As previously noted, destructive bombs were successfully employed in the bombings of corporate offices in Manhattan. In each case, the bomb was placed inside the plumbing access crawl space located behind restroom walls. The access doors to these spaces had not been secured. Seals can be applied in lieu of locks to secure access doors. However, compared to locks, they are relatively easy to force and could result in an excessive number of false alarms if curious or malicious people destroy the seals. An unobtrusive "seal," such as a matchstick placed in a door (a device well known to police) may be useful in routine checking of unsecured access doors.

Furniture. Waiting rooms, lobbies, and cafeterias too often provide a bomber with an area which is easily accessible and contains a variety of places to conceal a bomb. Figure 5 illustrates a typical lobby in which a device could be easily, quickly, and unobtrusively placed behind curtains which conveniently extend to the floor, inside large ashtrays or planters, and behind or under overstuffed furniture with decorative aprons.

Furniture can be rearranged and if possible, replaced, as shown in figure 6, to eliminate concealment possibilities. It is best to place furniture in conversational groupings or clusters around the room which are located away from wall surfaces. The new trend in furniture design makes bomb placement difficult. By purchasing contemporary steel tubular and plastic chairs it is virtually impossible to hide even a small bomb in the chair itself because there are no cushions and the chair is largely tubular open space. Clear plastic or glass accent pieces such as glass-top tables, plastic or plastic-wire trash containers, and clear ashtrays will increase room security. Draperies should end twelve inches off the floor, and all doors should be glass. The area should be sufficiently lighted so that there are no shadowed or darkened spots.

Public Area Surveillance. The adequate surveillance of public areas poses several problems. A posted guard will always have his back toward some section of a room and he may be easily diverted by the bomber's accomplice asking him a question or creating a diversion. The surveillance methods used by stores against shoplifters are also effective for observing areas for bombing activities. Attention can be focused on the placement of an item in the area by using concealed, closed circuit television units in conjunction with a posted uniformed guard. Other possible protective alternatives are plain-clothes guards, a two-way mirror observation post, or vision slots which are used in gaming rooms in Reno and Las Vegas. The posted information that such systems as closed circuit TV and/or vision slots may be present in a public area is in itself a psychological deterrent and the illusion may be further enhanced by the installation of several dummy lens units or mirrored surfaces on the walls near the ceilings.

The janitorial force is an important link in the security network. Because of the nature of their duties, they become intimately familiar with areas and items not normally inspected during normal operations. Disturbance or modification of such areas is frequently easily noticed by the janitorial force in their cleaning of public areas and during the removal of the day's accumulation of trash. With proper motivation and training, the janitorial force can become an additional 'round-the-clock element of the security force and should be included in overall planning of security operations.

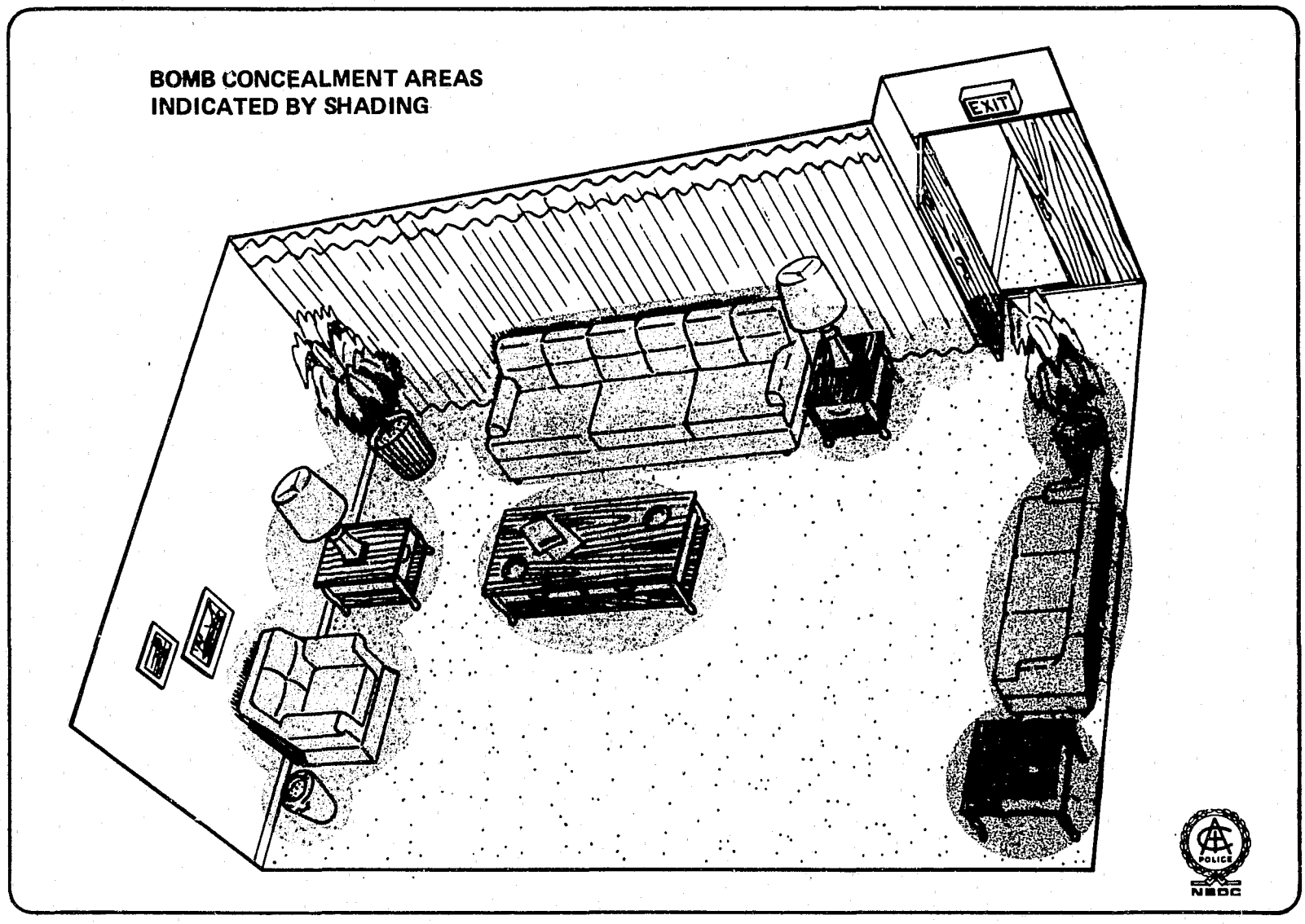

Figure 5
LOBBY WITH MULTIPLE AREAS FOR DEVICE CONCEALMENT

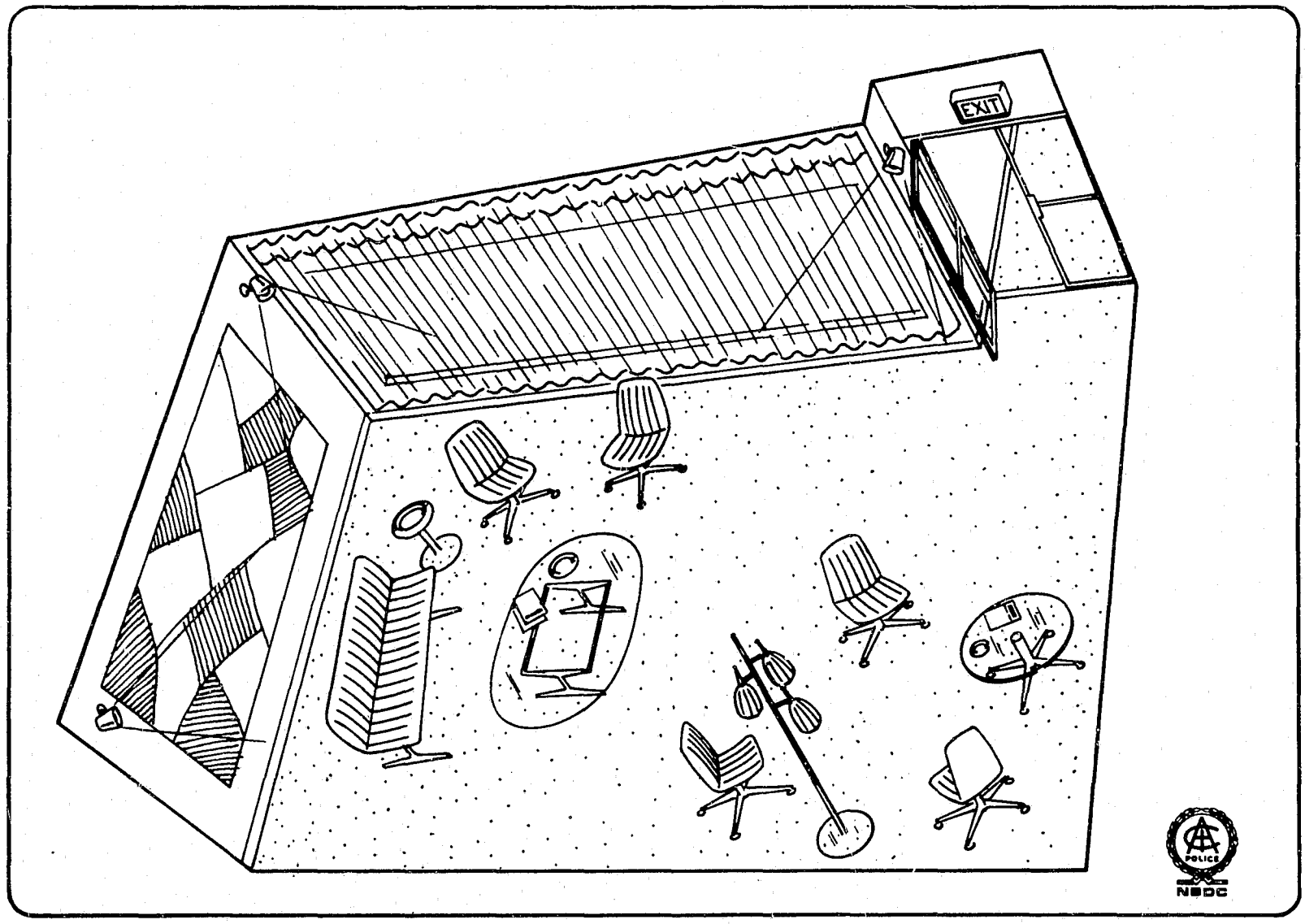

Figure 6
LOBBY REARRANGED AND REFURNISHED TO ELIMINATE BOMB CONCEALMENT AREAS

Motor Vehicles and Parking Areas. Motor vehicles, which are often parked or stored in areas open to the public, have become frequent targets of bombers in the United States. Bombing attacks on motor vehicles can be reduced through denial of access, the same principle recommended for buildings, but this is difficult to accomplish for public safety or service vehicles which must be parked unattended on the public street. A bomb prepared elsewhere can be installed in an automobile in a matter of seconds and even entry into the passenger or engine compartment is not always necessary. For example, the bomber can place his bomb under the vehicle, or attach it to a concealed part of the machine by using a magnet as illustrated in figure 7.

There are many ways to bomb an unattended vehicle. Some devices are designed to detonate after a given time, while others will only explode as the result of a specific action, such as opening a door, turning on the ignition, or starting the car in motion. Devices intended to kill or injure are usually placed under the hood and wired into the ignition system. Those bombs aimed at property destruction are most commonly put under the vehicle. One technique is to place "fireflies," metallic sodium-filled capsules in the gas tank. When the capsules dissolve, the metallic sodium comes in contact with the water content in the gasoline and produces a violent reaction of flame, shock, and pressure. Immediately, the gasoline tank ruptures and the fuel ignites.

Adequate security of vehicles is difficult to achieve. An experienced criminal can unlock standard door locks in a matter of seconds. "Anti-theft" door knobs have been designed without the protruding top, which cannot be released with a coat hanger or hook. Existing door lock knobs can simply be unscrewed and replaced with the straight knobs which are available for less than a dollar for a set of two at most auto-supply stores. The addition of a gascap lock and a clockspring-type

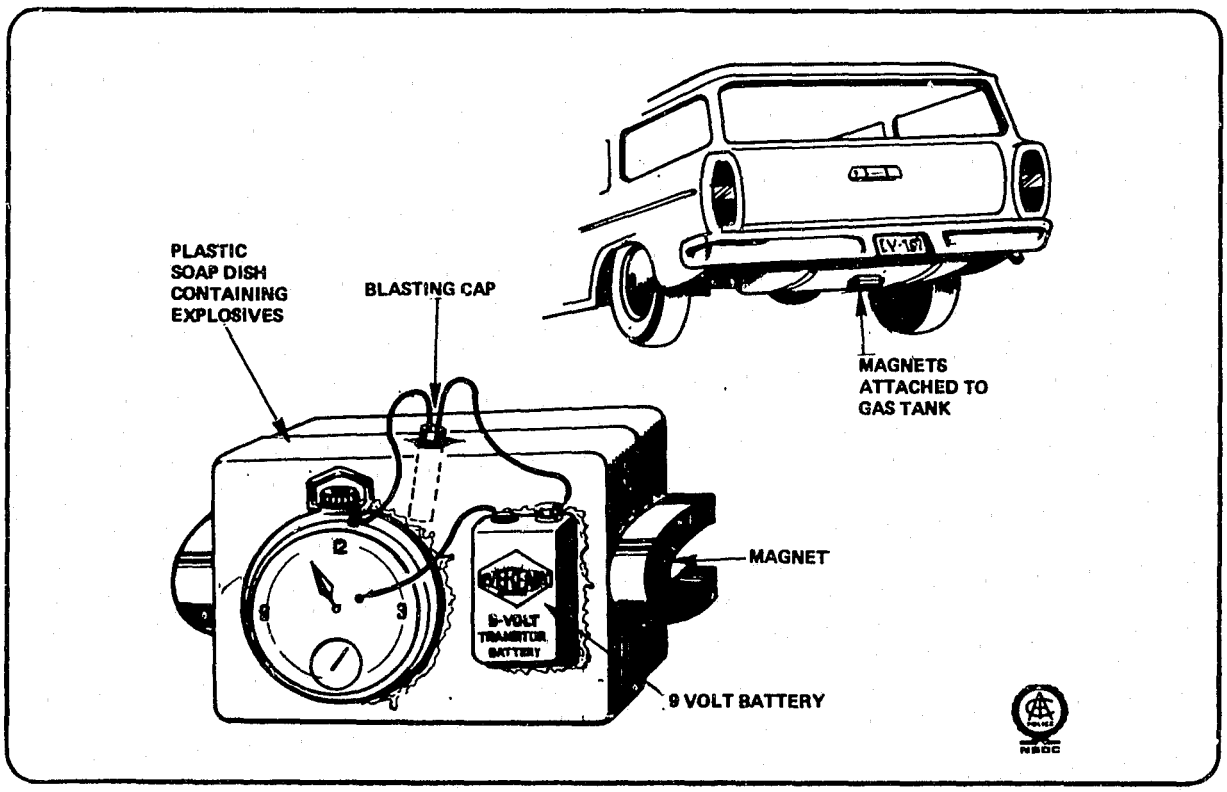

Figure 7
MAGNETIC ATTACHMENT OF BOMB TO GASOLINE TANK

anti-syphon device in the fuel filler pipe will deter the insertion of "fireflies" in the gas tank. Hood locks can delay a bomber from using the electrical system of the motor as a power source, but there are other unprotected, available sources of electricity such as the ignition and headlight switches. The use of all installed locking devices is recommended whenever a car must be left unoccupied.

Vehicles, which are considered possible targets for bombers, should never be left unattended in public parking spaces, and they should be parked in protected lots or garages whenever possible. Personnel and vehicle access to these parking areas can be controlled by using an identification badge or sticker system. Additional security can be provided by taking specific physical measures such as the installation of fencing, adequate lighting, LLTV* with moving image sensor, or electronic intrusion detection devices, and using security patrols or guard dogs.

Parking facilities should be located at safe distances from critical areas to avoid damage from a fire or explosion involving a vehicle. In all cases, vehicles should be parked in a manner which will insure their prompt removal in case of a fire or other emergency and which will allow continuous observation by guard personnel.

Boating Areas. Like vehicles and parking areas, boats and piers can be protected on the landward side by the use of security fencing, protective lighting, identification badges, package inspection and by the application of the various security measures described in this publication. Other measures are necessary to secure that portion of the pier which is accessible from the water, i.e., the pilings, the sides, the end, and the underside. Lights may be installed to illuminate the deck of the pier and the underside. Foot patrols may be used independently on the pier, or they may work in conjunction with boat patrols to prevent access to the pier by unauthorized craft. If circumstances warrant, it may be advisable to use booms and nets to protect the pier from small boats. A cable net may be suspended from the boom to deny underwater access. Fortunately, boats have not as yet assumed the importance of motor vehicles as targets for bombing attacks although Cuban refugee group bombings of ships in the Miami and Gulf port areas presented a major, but localized, security problem only a few months ago.

Utility Areas

Most buildings contain vital facilities which, if seriously damaged by a bomb, could result in the building being closed. These critical areas include:

- *Transformer vaults,* and the switch gear for these vaults if located separately.
- *Mechanical spaces* which contain boilers and air-conditioning units.
- *Machine or fan rooms* which house the distribution system for air.
- *Electric power* access points.

In addition, there are other areas or equipment which management officials may classify as critical, such as a water tower, a computer bank, or the communications center in a police station.

The security of critical areas and equipment is vital and warrants detailed attention. In addition to doorways, all openings, ducts, and adjacent areas must be examined with special care.

Electrical power units for the building or plant should be surveyed. If power is from a commercial source, it should be determined whether the power enters through underground cable

*Low light television.

or overhead lines. The location of primary transformer stations, the location of substations, and the adequacy of protection for all these points against bomb attack should be determined.

A successful bomb attack against a building transformer could be especially devastating. Similarly, damage to the distribution lines into the transformer or to the service connection from the transformer would result in a complete power loss. Repairs could take days.

The transformers which serve a building are generally located in underground vaults, in an outside building, or on a concrete platform near the building served. Underground vaults are often covered with a heavy grille to facilitate the dissipation of heat and are usually accessible by removing a manhole cover which leads to the vault. Entrances to transformer vaults and buildings which house transformers should be secured and the locks changed frequently. Security fencing should be erected around the areas, protective lighting installed, and the area patrolled. The use of sentry dogs and intrusion detection devices may be warranted in some circumstances. Because of the problem of heat dissipation, the use of sandbags to protect transformers from blast and fragmentation effects is impractical, with the possible exception of platform installations where adequate cooling can be maintained.

Distribution lines and service connections should be located underground and the drawings which detail the route of feed should be protected from unauthorized personnel. Where use is shared, a cooperative security program must be developed and implemented.

Pipelines and powerlines considered vulnerable to bomb attacks can be protected through surveillance by air, motor, horseback, or foot patrols. Local inhabitants of the area traversed by the lines should be recruited to observe, record, and report details of suspicious activity or strangers in the vicinity. If circumstances or intelligence reports indicate the possibility of an attack against a specific section of the pipeline or powerline, a guard force may be required to protect that point.

If regular or emergency power is generated on the premises, the level of protection should be examined. Emergency power, whether generated or stored, cannot be relied upon unless it is tested periodically. A weekly test would not be too frequent. It is also a sound procedure to test each of the systems which are powered by an emergency power source, such as emergency lighting, fire alarm systems, and communications.

Doors to electrical, mechanical, and machine rooms, as well as other critical areas, may be found to have been propped open, perhaps providing an opportunity for the bomber to gain access to a critical area. These doors should be periodically checked and, if necessary, signs posted which remind personnel to keep them continually locked.

ACCESS DENIAL

Every potential bomber is faced with the need to place his device in the target area. In the context of current bombing activity in the United States, this generally means that the explosive or incendiary device must be hand-carried and deposited at the point of detonation or ignition.[3] Thus the risk of bomb attack is substantially reduced if the bomber can be prevented from gaining access to the target location. As a practical matter, this can be achieved by denying access to unauthorized personnel and carefully screening or controlling the activities of those personnel with legitimate access. This section will briefly discuss several security measures that can be applied to deny access.

[3]This is not to deny the possibility that an explosive or incendiary device could be dropped from an aircraft, mailed, or projected from a distance, but only to recognize the nature of those tactics presently being employed.

While it is certainly true that access denial may be easier to achieve in an industrial or military setting than in a downtown office building, it is often surprising to find that access denial can be successfully employed to protect critical areas in even those buildings open to the general public. Any measures which limit the number of places where a bomb can possibly be concealed will reduce searching time and increase the probability that the device can be located before it detonates or ignites. Thus, denial strategy must not be overlooked, regardless of the nature of the facility to be protected.

Perimeter Barriers

A restricted boundary must be set around the entire area to be protected. Ideally, the security perimeter should be protected by natural or structural barriers, such as fences or walls. With the addition of illumination, intrusion detection devices, dogs, and guards, the perimeter barrier becomes a relatively effective defense against unauthorized access. In normal applications, the perimeter barrier serves several security purposes, including:

- Definition or identification of the security area.
- Control of authorized access.
- Denial or delay of unauthorized access.
- Psychological deterrence.

However, for buildings or entire facilities that are open to the general public for at least part of the day, the perimeter barrier loses much of its value, and security planning must develop denial procedures for certain selected areas during "open" periods and revert to the perimeter concept during "closed" hours. Where no external barriers are possible, the external walls of the building become, in effect, the security perimeter and methods must be devised to prevent or discourage the placement of bombs against the perimeter, since in this case the barrier is part of the protected target.

Fencing. Whether used as perimeter barriers or protection for internal critical areas, fences offer several security advantages. They define the security area, reduce the number of security personnel required, and facilitate the deployment of security forces. Although they cannot guarantee complete denial of access, fences will *delay* entrance to an area, and may serve as a psychological deterrent to a potential intruder. Also, fences will channel the flow of traffic and personnel to those points controlled by guards. Chain link mesh is the most commonly used fencing material. It permits the most effective use of security patrols in that surveillance of the exterior area is possible at all times. However, it also provides the potential bomber with an opportunity to study patrol schedules and to select the most advantageous time for a penetration attempt. Military-industrial security recommendations for chain link fence installations include:[4]

- Minimum height of chain link portion—4 feet.
- Number 11 gauge or heavier wire.
- Mesh openings not larger than 2 inches square.
- Twisted barbed-wire selvage—top and bottom.

[4]*Industrial Defense Against Civil Disturbances and Sabotage*, Office of the Provost Marshal General, Department of the Army, 1969.

- Extended to within 2 inches of firm ground or below the surface if soil is sandy and easily windblown or shifted.

- Fence mesh should be drawn taut and securely fastened to rigid metal posts set in concrete. Additional bracing, as necessary, should be placed at corners and gate openings.

- Topped with a 45 degree outward and upward extending arm bearing 3 strands of barbed wire stretched taut and spaced to increase the vertical height of the fence by approximately 1 foot.

- Provided with culverts, troughs, or other openings, where necessary, to prevent washouts in the barrier. If such openings are larger than 96 square inches in area, they should be provided additional protection.

- Checked (inspected) periodically for undergrowth, damage or deterioration.

Recommendations for masonry walls used as perimeter barriers include:

- Minimum height of 7 feet topped by a barbed-wire guard as described for chain link fence *or*

- Minimum height of 8 feet topped by a layer of broken glass set on edge and cemented to the top surface.

The length of time a fence delays an intruder determines the value of the fence. Alone, a fence is not a major obstacle and it is usually necessary to incorporate additional features which will increase its security value. Various features which may be added to make penetration more difficult include:

- Changing or rotating locks frequently.

- Constructing a perimeter road parallel to and inside the fence to facilitate the use of vehicular patrols, if the fence surrounds a large area.

- Guarding the fence.

- Installing intrusion detection devices in conjunction with the fence system, or parallel to it.

- Installing parallel fencing.

- Employing sentry dogs between parallel fencing.

- Installing protective lighting.

- Establishing clear zones surfaced with a light colored material, such as white sand, to provide better visibility.

Clear Zones. Whenever possible, clear zones free of structures, trash containers, vegetation, or other objects which will provide concealment, should be established on both sides of a security

fence. For maximum security, the clear zone should extend 20 feet outside the fence and 50 feet inside the fence. Grass in the zone should be cut whenever necessary to assure that it will not conceal a prone person. Clear zones should not be used for temporary storage or parking.

Underground Access. Many buildings are constructed with an underground channel or tunnel to accommodate utility pipes and conduits. Some are large enough to enable maintenance personnel to enter to adjust, repair, or replace equipment. It must be determined if there are exterior access openings to these channels. Interior openings, finished in the decor of the building, may be overlooked unless drawings are studied, or a building engineer consulted. These openings, as well as sewage or drainage pipes, should be protected against personnel or bomb access by physical security measures at the point where such channels pass under the perimeter barrier.

Doors and Windows

Locks and key controls for doors and windows in critical areas, exterior doors, electrical controls, elevators, and other potential target areas should be examined regularly. Security personnel must have a basic understanding of the characteristics of locking devices, principles involved in their installation, and especially the degree of protection afforded by different kinds of equipment.

All keys should be accounted for. Controls should be provided for issuing keys only to authorized personnel, and for securing keys when they are not in use. Biting numbers should be obliterated from keys to eliminate one means of duplication; and, if practical, the removal of keys from the building should be prohibited. The loss of keys and their removal from the building can be prevented by placing them on a heavy ring about 12 inches in diameter. The ring, which is welded closed, must be retained in the personal custody of an authorized person unless otherwise adequately secured. The addition of heavy swivels between the ring and the key may be necessary to prevent key breakage.

If the latch bolts in door locks are beveled, they should incorporate an automatic dead bolt feature. Otherwise, it may be possible to insert a metal or plastic strip between the door and the door frame and pull or push the latch bolt out of engagement by applying pressure to the beveled edge. However, automatic dead bolt locks may not always function properly. For example, the dead bolt may extend into the latchway (strike) with the latch or, in the case of double doors, it may be possible to force the locked door open by applying pressure until the automatic dead bolt extends into the latchway. Either way, it then becomes possible to use a metal or plastic strip to engage and open the latch bolt.

Any gap between the door and the door frame may be considered a hazard. Such gaps should be eliminated in the area of the lock by such means as mortising a metal angle bar into the surfaces of the stop and jamb, if the lock has a beveled latch bolt. On wooden frame doors with large gaps, locks with double-throw dead bolts, or bolts with at least a 2-inch throw are recommended to prevent the door frame being spread to disengage the bolt.

If new locks are to be installed, the dead bolt type is recommended. This type of lock requires the use of a key to lock and to unlock, and the retangular bolt cannot be manipulated by use of a metal or plastic strip.

On doors to machine rooms, and other critical areas having dead bolt locks, the addition of a spring-loaded hinge is recommended. This will keep the door standing open from 1 to 3 inches if the door is not locked, and enable security personnel to quickly identify doors that have not been secured.

Exposed hinges on doors to critical areas should have a nonremovable hinge-pin feature for good security. The same purpose can be accomplished by spot-welding the end of the hinge-pins to prevent their removal.

Numerous bombs have been placed at the entrances to buildings. In high-risk areas, the installation of overhead rolling doors (not grilles) of heavy steel may be considered for personnel and vehicle entrances. If motor driven, attention should be given to the location of the control switch and some means provided for protecting these switches and the power supply from unauthorized persons. If overhead rolling doors of heavy steel are installed, provisions should be made for a comparable level of protection in mounting fixtures. For example, heavy steel channels embedded in concrete may be appropriate.

If the public has ready access to the interior of a target building, it may be assumed that attempts to plant an explosive device will be made from within the building. However, if security procedures can effectively limit access to the building interior to authorized persons, an attack against the exterior of the structure or an attempt to throw a bomb through a window should be anticipated and proper precautions taken.

Bombs are frequently placed against or thrown through windows. This leads to a consideration of methods for providing protection against thrown bombs and the hazard of blast-shattered windows. To protect window areas, the following methods have proved effective:

- Installation of heavy grilles, shown in figure 8.
- Removal of window or building ledges, beveling or installation of angled metal siding to prevent bomb placement on ledges, illustrated in figures 8 and 9.
- Installation of a material such as "Lexan", a transparent synthetic resin developed by General Electric company in place of glass. This material resists both shattering and fragment penetration.
- Installation of heavy-duty laminated plate glass. This glass has exceptional resistance to fragmentation but can be broken with relative ease.
- Sealing up existing window openings.

The last method has an important disadvantage. If a bomb explodes in a room where the windows have been bricked up, personnel injuries and property damage may be more severe than in a room where windows permit venting and consequent dissipation of the explosive force. If the decision is made to brick-up existing windows, the construction should be equal in blast resistance to that of adjacent exterior walls.

A technique commonly used in areas where explosive or incendiary bombs are thrown through windows is to protect the first and second floor windows with screens of heavy expanded metal welded to frames. These screens are securely fastened to the building.

"Lexan" windows, heavy duty laminated plate glass windows, or bricked-up windows, expanded metal screens, angling of window ledges and overhead rolling doors if properly engineered and installed, may also be useful in the event of riots and civil disorders.

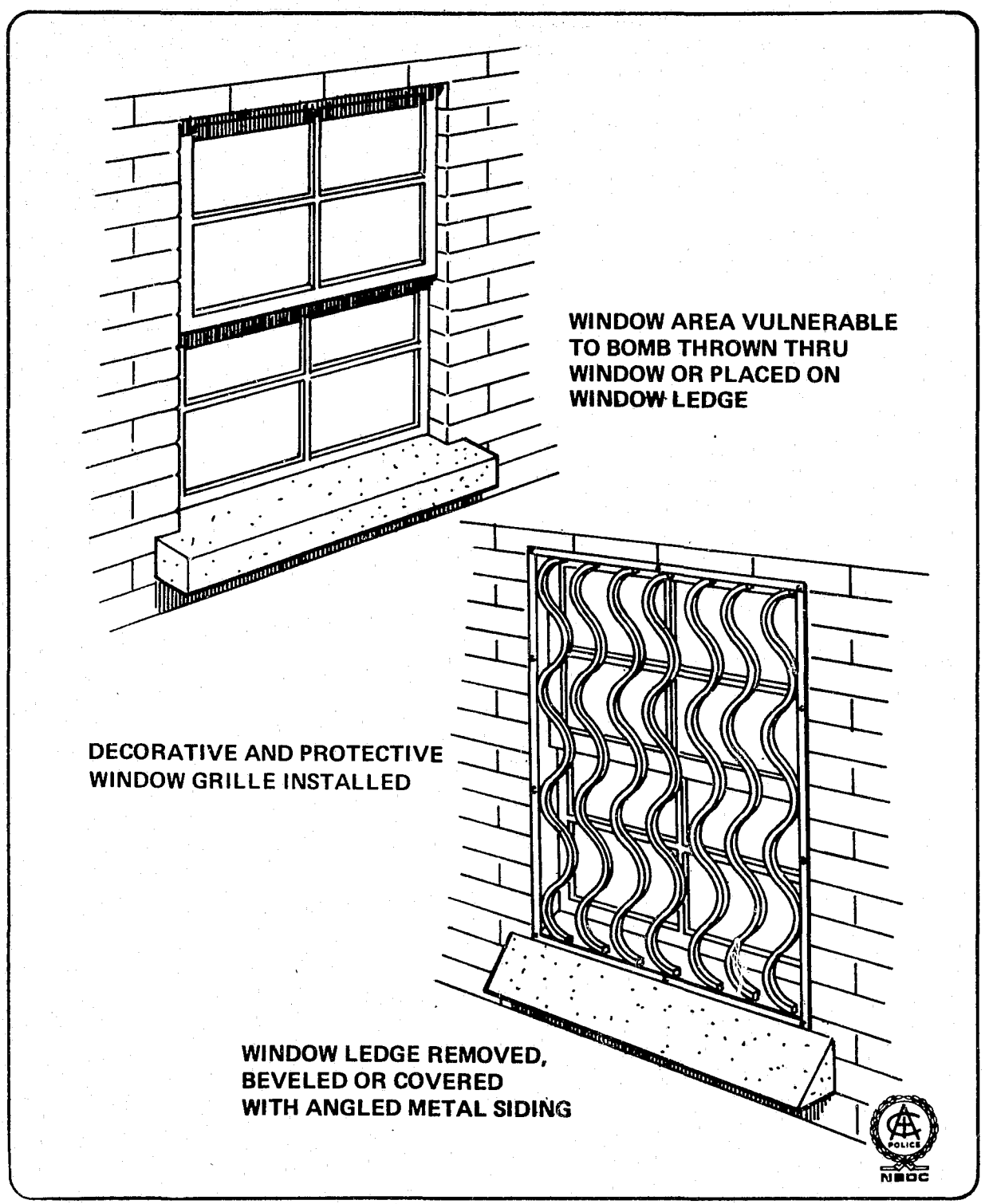

Figure 8
STRUCTURAL MODIFICATION OF WINDOWS

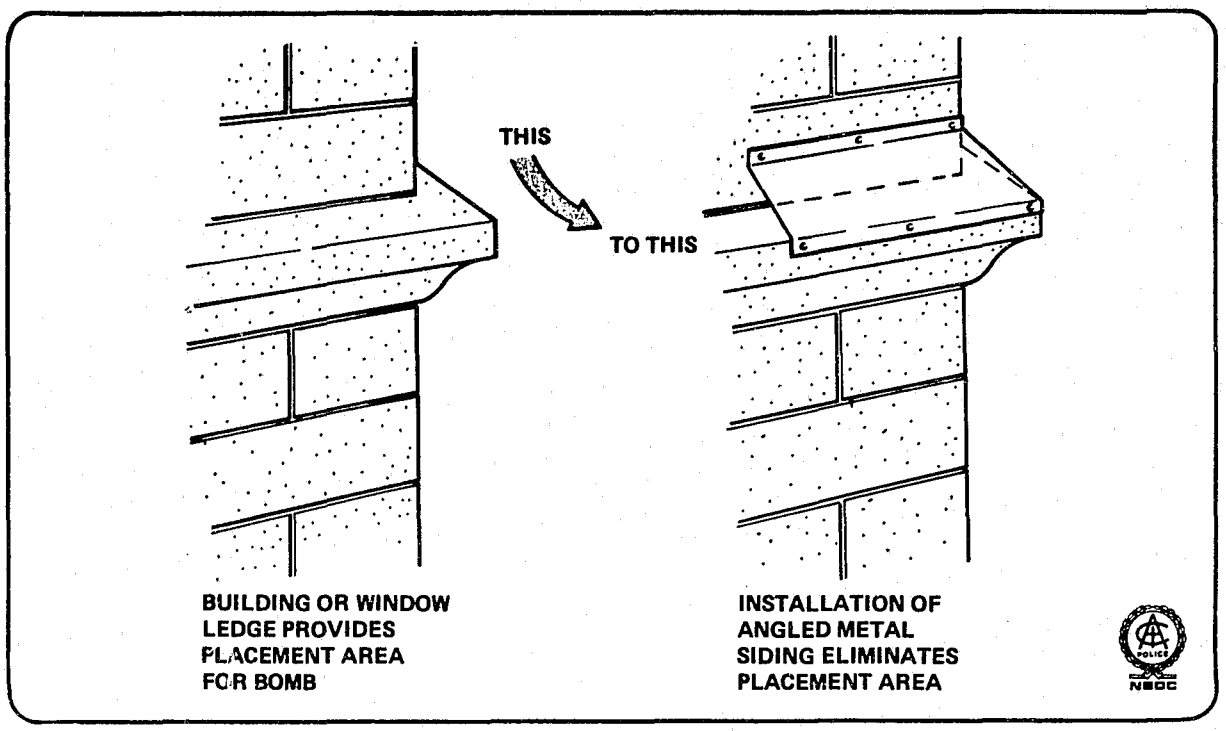

Figure 9
STRUCTURAL MODIFICATION OF WINDOW AND BUILDING LEDGES

Illumination

Outdoor protective lighting of several types will serve as a deterrent to the bomber and will enable security guards to observe the area without disclosing their presence.

Continuous lighting, the most common type of security illumination, consists of a series of fixed units which cover an area with overlapping cones of light. Figure 10 shows lighting placed at ground level against the building which vertically and horizontally illuminates a 90 degree area outward from the building and is now in use in some institutions. This type of lighting allows quick maintenance due to its positioning.

Command lighting is similar to continuous lighting, but is turned on manually or automatically if suspicious activity is detected.

Movable lighting, which is portable.

Emergency lighting, which may duplicate any or all of the systems described, and which has an independent emergency power source.

All lighting should be inspected regularly to determine cleanliness, serviceability, adequacy, and security of controls and circuitry. Lamps in protective systems should be replaced when they have been in use approximately 80 percent of their rated life. This will prevent dark spots in the perimeter lighting due to unexpected lamp failure.

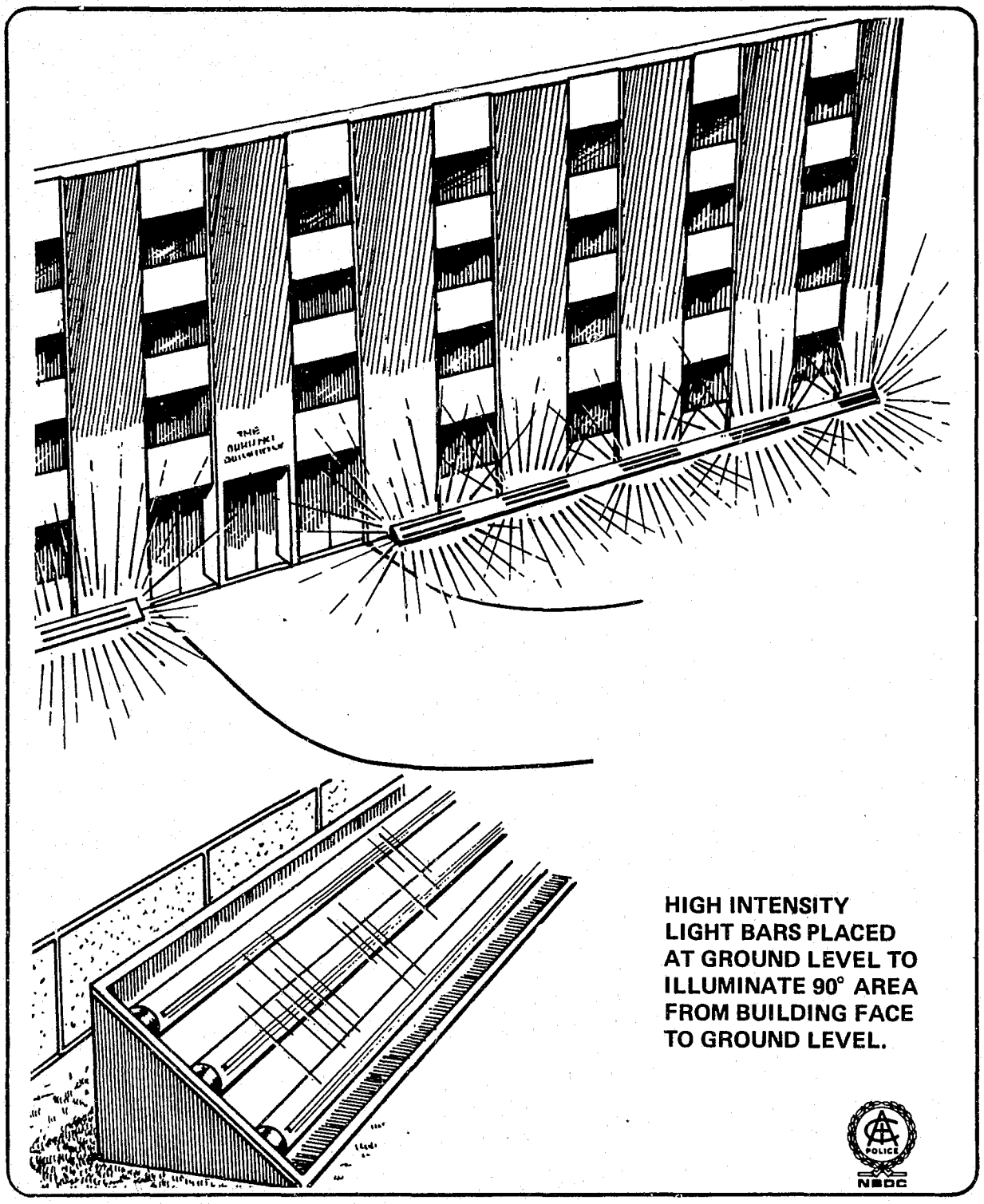

Figure 10
GROUND LEVEL AREA LIGHTING

Light fixtures can be protected by installing tempered glass lenses or wire guards and by placing them on metal poles with protected internal wiring. When consideration is being given to the installation of new protective lighting, the local power company should be consulted for recommendations.

Super bright indirect lighting installed in stairwells, public restrooms and utility areas will eliminate dark corners and act as a deterrent to illegal activity. A string of 150-200 watt lightbulbs strung down inside an elevator shaft acts as a deterrent factor to a potential bomber by making his actions visible.

Alarms

An intrusion detection alarm system is designed to *detect,* not prevent, an intrusion or attempted intrusion. An alarm system, to be of value, must be supported by personnel who can respond to the alarm in sufficient time and strength to prevent the delivery of a bomb or to implement emergency procedures if a bomb is found.

Four types of alarm systems are in use today:

- *Local Alarm Systems.* The responding or alarm device is located in the immediate vicinity of the protected area. Examples of these systems are in common use at small retail establishments such as drug stores and filling stations. Local alarm systems are usually simply designed and easily defeated. They often rely on bells or other audible alarms to frighten intruders, or alert neighbors or passersby to call the police.
- *Central Station Alarm Systems.* The responding or alarm device is relayed to a central station. The station system may be advantageous to establishments which require a higher degree of protection than that afforded by a local alarm system. Upon receipt of an alarm, the central station will telephone the police and request that a patrol unit be dispatched to the source of the alarm. Some commercial central station companies may also send their own patrols to the scene. All Underwriter's Laboratories approved central station systems have guard response available.
- *Proprietary Alarm Systems.* The responding or alarm device is relayed to a central location which is owned, manned, and operated by the protected organization. The alarm may also be relayed to local police or fire stations. The proprietary alarm system can be successfully employed by any organization large enough to maintain its own response force.
- *Direct Connect Alarm Systems.* The responding or alarm device is carried only to an alarm annunciator in a police station.

All alarm systems are comprised of (1) a detection unit, (2) the transmission system—which transmits the signal to (3) the responding or alarm device. The transmission system is the weakest link in the chain because it is most vulnerable to attack and most difficult to protect. Good security systems have provisions for automatically checking circuits and activating an emergency signal in the event of a line or component failure. Better systems have a feature to guard against the kind of tampering which does not cause an actual short circuit or broken connection, as well as against attempts to measure signal strength, circuit resistance or other properties. Additional protection can be obtained by using a system which features an alternating current signal superimposed on the normal direct line current or one which uses a digital system.

To be effective and reliable, each system should:

- Be capable of operating from a built-in power source in the event of a commercial power failure.
- Be tested at least daily.
- Be serviced by scheduled maintenance personnel.
- Be protected by keeping all plans, wiring diagrams, and specifications which pertain to the system secured at all times to prevent access by unauthorized personnel.

In selecting an alarm system or systems, there are various considerations. These include:

- The application (interior or exterior).
- Weather conditions.
- Ambient sound level.
- Building construction.
- Sources of vibration (subway trains).
- Existing sources of movement within an unoccupied room (forced air system).
- Radio and electrical interference.
- Cost (to include installation, maintenance, purchase vs. lease).
- Warranty and availability of service.
- Frequency of nuisance alarms.

Salesmen's claims do not always correspond with users' experiences. Therefore, it is suggested that advice on alarm systems be solicited from persons or organizations who are using security alarm systems in comparable situations. The main characteristics of alarm systems are summarized in figure 11.

Any alarm system which generates frequent nuisance alarms may lead to a casual response to alarms by guards. However, it should be noted that attackers may activate numerous alarms in an effort to determine the response time of security patrols and to condition the patrols into thinking that each alarm from the station is a false one. Security patrols must be trained to respond promptly to each alarm, prepared for any emergency. To be effective against the potential bomber, guards or police must respond to an alarm in sufficient time to prevent the activation of the explosive or incendiary device.

Activation	Advantages	Disadvantages
Breaking an electric circuit	Most trouble-free service; few nuisance alarms; used on doors, windows, ducts, temporary walls	May be defeated by bridging circuits from within
Making an electrical circuit (Electrical pressure switch mats or runners installed under carpeting)	Operates on independent power supply—good for indoors use only	May be defeated by cutting wiring circuit from within
Detection of sound and vibration	Economical to install	Practical only where or when low ambient noise encountered
Interruption of light beam	Effective when employed within limitations, e.g., for detecting a large mass, such as a vehicle	Weather or vegetation may cause nuisance alarm; possible for person to avoid beam
Motion detection (an ultransonic sound pattern is disturbed)	Easily installed; relatively low maintenance	Effective indoors; but possible to by-pass by slow or low movement
Penetration of an electronic field (An intruder unbalances an electronic field)	Easily installed; high degree of protection	Limited range; nuisance alarms from moving objects, birds, etc.
Closed circuit TV (may include moving target indicator with video or audo signal)*	Provides good perimeter protection	Inclement weather may limit use; unless moving target indicator included—requires continuous surveillance

*May then be considered as components of an alarm system

Figure 11
CHARACTERISTICS OF ALARM SYSTEMS

Security Guards

Security personnel are an important element in preventing bomb attacks. Physically fit, properly trained, equipped, and supervised security personnel can respond to alarms on a timely basis and serve as an effective measure against bombing attacks. They can quickly recognize and report security weaknesses which they observe, and more importantly they will know what to do if they encounter a suspicious person or find a bomb or suspicious object.

Orders should be published in concise, simple language. They should define the limits of posts, prescribe specific duties, and set forth the authority of the guard personnel.

Various techniques may be used to supplant personnel supervision as a means of assuring that necessary areas are patrolled.

- *The Recorded Tour.* The recorded tour system provides "after the fact" type of supervision. The patrols are verified by examining the recordings in watchclocks that are carried by the security guards, or installed at various locations along the route.
- *The Supervisory Tour.* The supervisory tour system provides instantaneous supervision. As the guard starts his round, he inserts a key in a lock located at a tour station. This signals the console and records the information. The procedure is repeated at each tour station. If a guard does not signal the console from the next station within a predetermined period of time, or if the tour station is tampered with, an alarm will sound at the console.

All security guards should be required to report regularly to a guard control center and each report should be recorded. Failure of a guard to report as required, or any deviation from established reporting procedures should be immediately investigated. Patrol routes should be varied within prescribed limits. By rotating patrol assignments, and by making random patrols, guard activity will be hard to predict and the attacker's job will be made more difficult—and security increased.

Dogs. Sentry dogs can often be used effectively to supplement a guard force. If the dogs are used within certain limitations, they can serve to deter, detect, attack, or detain suspicious persons. Because of their keen sense of smell and hearing, sentry dogs can be advantageous during hours of darkness and inclement weather when the visibility of a guard is limited. A dog is capable of detecting a sound at 26 yards which is inaudible to a human at 6 yards.

The most common method in which a sentry dog is used is as a member of a sentry dog handler team. With this method, the leashed dog accompanies the handler during his patrols. If the dog detects an intruder in or near the protected area, he will alert his handler.

There are other ways of utilizing sentry dogs:

- They may be placed in a building after working hours and removed the following morning.
- They may be placed in areas between a double security fence.
- They may be leashed to a cable which extends between two locations.
- They may be chained at a specific location.
- They may be placed in a vehicle.

When the sentry dog is used without a handler, the dog will alert the guard by barking if an intruder is detected in or near the protected area. A dog can be most effectively utilized in isolated and remote areas and during hours of darkness when there is little activity and noise, since distracting noises and activity will limit a dog's ability to detect an intruder. Dogs should be kept at a minimum of 75 yards from areas of personnel activity and should not be worked near roadways. The dog's ability to smell is inhibited by the odor of petroleum products, making assignment to such an area unsuitable.

In addition to performing security patrols and inspections, the guard force normally performs those personnel, material, and vehicle control functions discussed in the following section.

IDENTIFICATION AND MOVEMENT CONTROL

Identification and movement control techniques are intended to prevent the entry into protected areas of unauthorized personnel, materials, or vehicles by imposing security measures that screen and control authorized access.

Personnel Control

The key to personnel control is identification. The access control system, whether human or electronic, must have some basis for making highly reliable decisions about whether or not an individual should be allowed to enter a protected area. The effectiveness of the security program will depend upon the accuracy with which identification decisions are made and the diligence with which the system is applied. The best personnel identification procedures are useless if carelessly or sporadically executed.

Personal Recognition. The best method of positive identification is that of personal recognition. Unfortunately, it is not practical in those situations where the number of employees or occupants using an entrance exceeds about thirty. To be effective, a personal recognition system should be used only when personnel turnover is low and guards should be trained and tested to insure their ability to recognize authorized personnel. Naturally, a method must be implemented for notifying guards of personnel who are no longer authorized entrance through their posts.

Passes or Badges. Where personal recognition systems are impractical, an artificial identification system employing passes or badges can be used. Although badges and passes may incorporate a variety of security features such as photographs, expiration dates, serial numbers, coding systems, authenticating signatures, and deterrents to alteration, they are still subject to loss and theft, and some to alteration or reproduction. As soon as a pass or badge is lost or stolen, the system is compromised and depending upon the degree of security desired, it may be necessary to replace all passes or badges.

In addition to the control of badges and passes themselves, consideration must be given to control of badge and pass components. This should begin with the manufacturer, where the same safeguards should be applied to badge components as afforded other valuable or negotiable documents such as city tax receipts and automobile registration forms. A person should be designated for the receipt, safekeeping, issue, and destruction of both badge components and badges. A permanent record of all badges, and procedures for a periodic review of the record and for the inventory of badge and pass component stocks, is recommended.

There are at least three pass and badge systems that can be employed, again depending upon the degree of security sought.

- *The Single Pass or Badge System.* With this system, access to an area is authorized if the bearer displays a proper pass or badge in the manner prescribed by security regulations. The system can be expanded by use of a coding scheme in which a color or overprinted number or letter designates a shift or authorization for access only to specific work areas.
- *The Pass-Badge Exchange System.* The pass-badge exchange system is used to minimize the effect of lost badges. With this system each employee is issued a pass or identification card. A corresponding badge is retained at the gate or entrance. Both pass and badge include identical photographs, name of the employee and other identifying data. When the employee enters the area, he presents his pass to the guard. The guard compares the identification data and photograph on the pass with the appearance of the bearer. If there are no differences, he

removes the corresponding badge from a rack, replaces it with the pass, and hands the badge to the employee. The employee must wear the badge face up on his outer clothing so that it is clearly visible at all times. When the employee leaves the area, the procedure is reversed. For this system to be effective, the requirement for wearing the badge must be strictly enforced and rigid control of badges not in use is essential.

- *The Multiple Pass or Badge System.* To supplement the pass-badge exchange system, the multiple pass or badge system may be employed. With this system an additional pass-badge or badge-badge exchange is required for access to critical areas, thereby providing additional security.

If guards are used at entrances to control personnel access, there must be some means of physically directing the flow of personnel past the guard post in single file. There should be a communications system which will enable the guard to summon help, or a relief, if needed. Lighting at entrance positions should be adequate for guards to observe personnel, check briefcases and parcels, and examine the passes or badges of employees.

The practice of flashing a pass or badge at a guard should not be permitted when the risk of unauthorized entry is high, since the guard may not be able to fully inspect the access document. In such cases the person entering should be required to hand his pass or badge to the guard so that he can:

- Confirm that personal identification data matches the bearer.
- Determine that the pass or badge does not show evidence of tampering.
- Insure that the pass or badge has not expired.
- Check that the pass or badge is not carried on a revoked list.
- Verify that the pass or badge is legitimate for the time of entry and/or area to be entered.

In large plants, where hundreds of employees arrive at work about the same time, the procedure of scrutinizing badges is not practical. Instead, guards may be trained to scan large crowds, seeking out suspicious persons. Those, for example, who walk too rapidly or too casually, or who are overly friendly but unknown to the guard. When large numbers of employees are involved, all should be required to wear the badge, face up, so that it is clearly visible at all times. The coding system may be incorporated in the badge to optimum advantage in such situations. In addition, random and frequent inspections of badges both at entrances and internally will provide some security in dealing with large numbers of personnel.

Key Access. Personnel access to buildings or selected areas of buildings can also be controlled through the use of electronic or mechanical locking devices. For buildings with few occupants, the system commonly used to secure a private residence may be applied which has the refinements of key controls, the use of quality locks, and provisions for changing locks if a key is lost or stolen.

Combination locks, mechanical or electronic, are also available. These require that buttons or switches, mounted on a panel on or near the door, be pressed in the proper sequence before the latch will open without the use of force. Both types have provisions for changing the combination without the services of a locksmith. If electronic locks are used, attention to the possibility of power failure is warranted.

Some electronic models of the combination lock have a feature which activates an alarm, either locally or at the control center, if a person fails to press the proper sequence of buttons within a predetermined number of attempts.

Other electronic lock systems can be opened only by inserting a magnetized card. Sophisticated versions incorporate a provision for canceling a lost card, if reported, so that it can no longer be used in the system. An alarm may also sound, usually at the control center, if a person attempts to introduce a void or improper card into the system. More elaborate systems will record the details of each opening.

Any of the systems described for securing unmanned entrances have a common weakness, the possibility of an unauthorized person entering with an employee. For these systems to be effective, all employees must prevent unauthorized persons from entering with them and security measures must be taken to prevent an authorized individual from being forced to grant access to an intruder.

Visitors. Procedures for visitor control will depend upon the nature of the facility and the level of security desired. In any event, visitor control measures should be a balanced part of the total security plan. The following procedures can be used alone or may be combined to handle the movement and identification of visitors in a protected area.

- *Casual Screening.* Visitors can be permitted to enter protected areas if their stated purpose is plausible and the guard has no reason to be suspicious of their intent. This provides, of course, a low level of security.
- *Verification.* The guard may be required to first contact the person to be visited to determine the validity of the visitor's explanation.
- *Verification and Escort.* After verification, a guard or authorized employee escorts the visitor to his destination in the protected area. The escort must be maintained by guards or employees during the entire period of the visit.
- *Verification and Timed Travel.* With a timed travel visitor control system, the guard first verifies the visit and then informs the host that the visitor is en route, recording the time. Maximum and minimum travel times to different areas are predetermined. When the visitor arrives at his destination, the guard is informed by phone and the time again recorded.
- *Sign-in and Sign-out.* Visitors are required to produce identity documents and then sign-in on a visitor control log. The guard on duty should enter the time and date of entry and require that the visitor's name also be printed if the signature is illegible. Upon departure the visitor again signs and the guard enters the time.
- *Badges or Passes.* For frequent visitors it may be expedient to issue a permanent badge which clearly identifies the visitor. Badge controls, similar to those for regular employees, should be used. If visitor's passes are used, there must be a way of insuring that they are returned; otherwise, they are of little or no value. Procedures may be added which require the person visited to authenticate the pass. To be effective, the authentication procedure requires that specimen signatures be available to the guards

  Another method for identifying visitors is to issue a printed pass, about 7½ inches by 3½ inches, which is worn in the jacket pocket. Data is contained on only the upper 3 inches of the card stock. After three half-inch lines are provided for the date, the area, and the name of person to whom the pass is issued, a distinctive emblem or organization name, is included in the space remaining. The passes are date-stamped; in addition, the passes may be printed on various colors of card stock and colors changed daily on a random basis.

Vehicle Control

Parked vehicles have been used successfully to conceal bombs next to a target. In one incident a

truck loaded with oil-soaked commercial fertilizer was exploded by terrorists, killing one person and causing one-half million dollars damage to the target building.

If parking, standing, or loading zones exist on a street adjacent to the structure, or if vehicles are permitted into a security area or loading dock, the threat must be evaluated. Structural barriers may be necessary to prevent vehicles from being driven to vulnerable areas and additional blast protection may be warranted for critical areas where a vehicle containing an activated bomb could be parked.

If vehicle access is controlled at a gate, the risk of permitting essential commercial vehicles into an area can be reduced by:

- Insuring that all security personnel are familiar with the usual pattern of activity of commercial vehicles.
- Inspecting vehicles when entering the area.
- Maintaining a detailed log of vehicles which enter the area.
- Reviewing the log periodically to determine unusual patterns of activity.
- Providing an escort for each vehicle.

Material Control

While it is certainly possible to conceal a sizable bomb on the person or to conceal bomb components on several persons, experience indicates that most bombers carry or send the bomb to the target in some form of container. Thus, any reasonable degree of security requires the inspection or diversion of all incoming parcels, briefcases, and other containers.

Manual Inspection. Security personnel can manually open and inspect all incoming containers. This is time consuming and costly, but effective when practical. Unfortunately, in the case of public buildings, the legality of such searches is not clearly established and legal advice should be sought in each jurisdiction. Where volume precludes total inspection, random or spot checks can be conducted. Container inspections should be conducted by personnel trained in bomb and bomb component recognition. This is especially true of packages arriving in the mail or by delivery service, since they may be constructed to detonate when the container is tampered with in any way.

Radiographic Inspection. Radiography may be useful in detecting bombs concealed in packages and luggage. This method of inspection permits the examination of internal objects by viewing the shadows cast on a fluorescent screen by objects through which x-rays have been directed. Because of the radiation hazard, an optically transparent but radiographically opaque barrier must be placed in front of the screen. The hazard of x-rays also precludes the frequent use of radiography for searching personnel and requires the use of safety equipment to protect operators from overexposure. The size and content of the items which can be examined will be limited by the energy of the x-ray unit. Generally, x-ray or fluoroscopic inspection is used only for highly suspicious items which are not accompanied into the facility.

Package Diversion or Holding. The use of a package holding area, designed to provide protection against the blast of an explosive device concealed in a package, will facilitate the flow of pedestrian

traffic into a building by eliminating the requirement for conducting a search of each incoming package. The package holding area should be located near the building entrance and should be designed to protect the building occupants and contents against the blast of an explosion, by venting the blast through a frangible wall into an unoccupied area. Whenever possible, the holding area should be located in a separate structure.

SECURITY DESIGN CHARACTERISTICS

From the standpoint of bomb security, certain design characteristics of a building acquire added significance. In the planning of new construction or substantial remodeling, there is an opportunity to include design features which will result in increased physical security. Beginning with site selection, a location which provides a clear area around the structure will make hit-and-run attacks more difficult. The topography of the land and requirements for parking, loading, driveways, and other features may predetermine the conformation of a building. Whenever possible, however, a rectangular, unattached building which is positioned on a uniform elevation is desirable from a security point of view because it can be covered with fewer guards or television cameras than can a multi-sided building on different elevations.

Reinforced concrete is recommended for use in blast resistant construction since it can be fabricated in any part of the country. Also, a structural engineer can design reinforced concrete to protect against specified quantities of a given explosive.

Building surfaces at ground level should be devoid of recessed areas, alcoves, projections, or oversized columns. Where absolutely necessary, window wells should be protected with bars or steel grilles. Foliage and landscaping features should not be permitted to obscure the visual observation by guards or furnish places of concealment for explosive or incendiary devices.

Building Openings

Principal entrances and exits should be at or above the street or grade level to reduce the need for stairwells which make observation by a guard more difficult. If stairs are necessary, an open design is recommended which will facilitate observation and reduce bomb concealment opportunity.

By limiting exterior building entrances to the minimum amount needed for operational requirements, the number of guards required to control access through these entrances will also be reduced. Fire exit doors should have alarms and controls should be established to prevent their use except in an emergency.

The elimination or limited use of windows on the first and second levels above ground should be considered to prevent bombs from being thrown into the building.

Stairwells

Stairwells may provide an intruder with means of moving within a building undetected. The stairwells should be designed, subject to the approval of the local fire authorities, so that all stairwell doors can be locked to permit exit from the stairwell only at the ground level, but to permit entrance into the stairwell from all floors above ground level.

In modern construction, many fire codes require that buildings designed for office or similar occupancy have stairwells which terminate at the ground level. This prevents persons who use the stairwells during an emergency from bypassing the ground floor and continuing into a basement or sub-basement. When all stairwells exit or terminate at ground level, two stairwell entrances will be located side by side: one which leads to upper floors, and one which leads to lower floors. Many

designs make it possible for an intruder to climb from a basement stairwell into the stairwell which services the upper floors or to escape from a building by entering the stairwell from an upper floor, descending to the first floor, climbing over a railing into the basement stairs and using an emergency exit. This security hazard can be eliminated by the installation of a heavy, expanded metal cage or screen which will prevent climbing from one stairway to another.

Elevators

Elevators also provide a means for the undetected movement of personnel in a building. A common method of maintaining security against this is security programming. For example, elevators can be programmed to permit designated elevators to operate only from the first to the upper floors; others between the first and lower floors. With this programming in operation, all persons will have to change cars at the first floor who want to go to a floor which requires travel past the first floor. For example, if a person enters in the basement and presses the button for 10, the elevator will take him only to the first floor. Similarly, if an intruder is on the 10th floor and presses the button for the basement, the elevator will not go to the basement, but will stop at the first floor. Other variations of programming can be supplied by elevator manufacturers to meet specific needs.

The interior of elevator cars should be designed to eliminate indirect lighting wells or other receptacles where a bomb might be concealed. Ceiling escape or service panels should be equipped with alarms. Structures housing elevator machinery should be designed and constructed for security as well as utility.

Guard Stations

In a building where stairwell doors are located near the elevator lobby, the control of personnel movement within the building can be facilitated by constructing a guard station in the immediate vicinity on the first floor lobby to permit observation of both stairwells and elevators from a single point.

With security programming in effect, a person who enters an elevator on any floor other than the first, will not be able to bypass the first floor and will come within the range of observation of the guard.

Control over elevators can be provided by installing a system of lock-out switches inside the guard station. If a person attempts to bypass the guard and enters an elevator, the guard turns a key and the elevator is put out of service.

Additional security can be provided by using an elevator car indicator panel in the guard's station. If, for example, a person signs in with the guard during security hours for Room 1602, the guard watches the car indicator panel. If he observes that the car bypassed the sixteenth floor and did not stop until 22, the top floor, he notifies the control center and guards are dispatched to investigate.

Public Restrooms

Since public restrooms are a recognized bomb concealment hazard, consideration should be given to protecting adjacent areas and to designing them with a frangible wall which will vent a blast away from occupied areas. Again, any reduction in concealment areas will reduce search time and discourage potential bombers.

Rooftop Locations

Rooftop locations are recommended for the installation of air handling equipment, the transformer which serves the building, the transformer switch gear, and similar equipment, because of the relative ease of securing these locations. Rooftop locations for transformers pose a problem of replacement. However, transformers can be moved via freight elevators or by crane. Security of the access doors to these rooftop locations should include the installation of dead bolt locks and the use of electronic intrusion detection devices at all hours.

If guards are to be utilized in a rooftop location, provisions should be made so that the guard is not silhouetted against the sky during his tour of duty. Anti-silhouette devices should be installed on rooftop areas routinely patrolled, or used as observation posts by the security force. Such a device may be constructed from plywood sheets extending to a height above roof level sufficient to preclude the silhouetting of security personnel from the ground.

Figure 12 illustrates an installed anti-silhouette device which is both functional and decorative. An anti-silhouetting device further serves to conceal the location of rooftop air vents, air-conditioning units and machinery rooms and provides the guard force with protection from the elements.

Security of Design Details

The disclosure of the security features and drawings which pertain to a specific structure should be limited to those persons who have an absolute requirement for the information. The unauthorized disclosure of this information, or information such as the route of a distribution line from a substation into the transformer which serves the building will jeopardize the security of the building. Specifications, diagrams, and drawings which contain such information should always be secured when not in use.

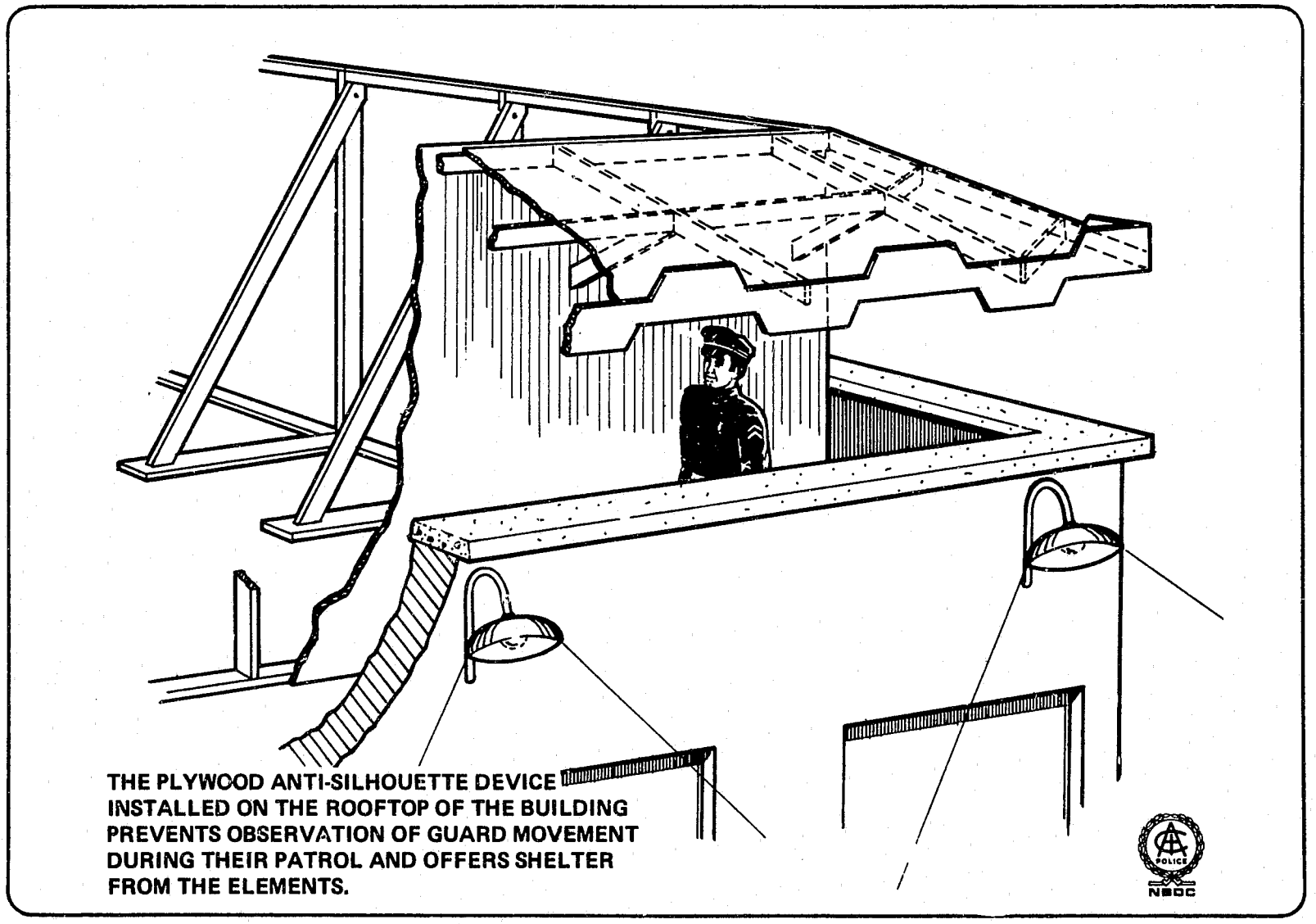

Figure 12
ANTI-SILHOUETTE DEVICE

APPENDIX A

BOMB SECURITY OUTLINE

This form is provided to serve as an outline or checklist of key bomb security measures discussed in this publication. As such, it can be used for planning or for a rapid security survey. Here again, no attempt has been made to incorporate the full range of physical security measures, only those steps especially appropriate to bomb security have been extracted.

PART I THE SECURITY PLAN

Plan Objective

☐ Prescribe security measures to prevent bomb attack; reduce danger to property and personnel in event of attack.

☐ Bomb incident plan, if not included in basic security plan.

☐ Provide orderly and efficient transition from routine to emergency conditions.

☐ Specify emergency responsibilities.

Execution Instructions

☐ Designate individuals to execute plan.

☐ Set forth conditions under which plan may be partially executed.

☐ Set forth conditions under which plan should be fully executed.

Control Center

☐ Protect.

☐ Control Access.

☐ Provide capability for receiving and recording all incoming communications on a timely basis.

☐ Train personnel; test.

☐ Issue center personnel brief, clear printed instructions which are authenticated.

☐ Provide emergency power for lights and communications.

☐ Plan for 24-hour operation, if not in effect.

Communications

☐ Within organization.

☐ With parent organization.

☐ With police/fire.

☐ With guards.

☐ Emergency power for above.

☐ Back-up systems, e.g., walkie-talkies, hold-up alarm, power megaphones.

☐ With employees away from organization.

☐ Test systems.

☐ Secure systems.

☐ Train personnel to operate.

☐ Maintain systems in good repair.

☐ Develop code for discreet announcements over PA systems.

☐ Monitor select police and civil defense networks.

☐ Establish radio communications with police and/or civil defense authorities.

Coordination

☐ With parent organization.

☐ With lateral organizations.

☐ With subordinate organizations.

☐ With emergency bomb disposal support organizations.

☐ With police officials.

☐ With fire officials.

☐ With FBI.

☐ With civil defense officials.

☐ With local utility firms.

☐ With emergency medical support actitivites.

☐ With telephone company.

☐ With employee relations.

☐ With legal counsel.

☐ With employees with emergency assignments.

☐ With guard force.

☐ With building engineers.

☐ With organization officials.

☐ With employees to degree necessary; do not alarm.

PART II SECURITY EDUCATION AND TRAINING

Employee Training Procedures

☐ Include in orientation of new employees.

☐ Familiarize all personnel with evacuation procedure.

☐ Explain pass procedures: where and when to wear pass, how to hand to guard, etc.

☐ Explain visitor's pass procedures.

☐ Instruct persons who might receive bomb threats (telephone operators, etc.) on action to take in such an event.

☐ Caution all employees to immediately report suspicious persons, objects, and vehicles: stress importance of noting distinguishing characteristics.

☐ If visitor wants to leave package or briefcase with employee, instruct employee to require visitor to first open the item for examination; if visitor refuses--summon guard.

☐ Tell employees to immediately inform guard if they see anything that does not belong or which is suspiciously out of place in the building or work area; caution on danger of touching.

☐ Instruct search team members how to search and what to look for.

☐ Train building operating engineers in the procedures for shutting off power, gas, and fuel lines which lead to danger area.

☐ Stress to all employees and guards that bombers may wear organizational uniforms or pose as telephone or utility company employees, to case an area or to plant a bomb; provide positive means of verifying the identification of visitors and the validity of their visit.

Train Guards In:

☐ Organization and functions of guard force.

☐ Authority and jurisdiction.

☐ Observation and description.

☐ Techniques of arrest.

☐ Use of firearms.

☐ First aid.

☐ Report writing.

☐ Communication systems.

☐ Alarm systems.

☐ Methods used by bombers.

☐ How to search for bombs and what to look for.

☐ Security fences and lighting.

☐ Building/area protection.

☐ Critical area protection.

☐ Public area protection.

☐ Personnel and movement control; pass and badge systems, access lists, etc.

☐ Patrolling.

☐ Challenging.

☐ Uniform and equipment.

☐ Uniform and equipment.

☐ Emergency duties.

☐ Public relations.

PART III PRIME TARGET AREAS

Critical areas

☐ Identify.

☐ Protect walls, ceilings, and floors which are vulnerable to attack.

☐ Protect critical equipment.

☐ Illuminate the entrances.

☐ Secure and protect all openings.

☐ Install dead bolt locks or rekey existing locks.

☐ Control keys.

☐ Install intrusion detection device.

☐ Use access list to control entry.

☐ Instruct occupants to challenge all visitors, maintenance personnel, etc.

☐ Provide for frequent patrol.

Public Areas

☐ Identify all areas where a bomb might be concealed.

☐ Eliminate all areas practicable where a bomb might be concealed.

☐ Secure as many of the remaining hazards as feasible.

☐ Provide for frequent patrols by uniformed personnel of public areas, which will include inspection of remaining hazards.

☐ Provide surveillance of public areas.

☐ Maintain doors to wire closets, mop rooms, service stairs, service areas, etc. locked and/or sealed.

☐ Lock or seal access panels to crawl spaces.

☐ Maintain good-housekeeping standards.

PART IV ACCESS DENIAL

Fences

☐ Inspect.

☐ Note need of repairs; report and follow-up.

☐ Provide clear zone.

☐ Remove objects which would assist in climbing.

☐ Rotate locks.

☐ Observe.

☐ Patrol.

☐ Illuminate.

☐ Maintain in good repair.

☐ Secure entrances when not in use.

Lighting

☐ Inspect; test.

☐ Determine adequacy.

☐ Clean.

☐ Repair.

☐ Replace burned out bulbs.

☐ Provide for bulb replacement after 80% of rated life.

☐ Secure conduit, controls, and power supply.

☐ Schedule periodic maintenance.

☐ Schedule periodic tests.

☐ Provide emergency power source.

☐ Schedule and execute periodic tests of emergency power source.

☐ Provide for scheduled maintenance of emergency power source.

☐ Secure emergency power scurce.

☐ Instruct guards to report burned out bulbs.

☐ Instruct guards to challenge personnel who service or maintain lights, conduits and controls.

☐ Provide adequate lighting for indoor patrol routes.

☐ Obtain and maintain emergency lights.

Alarm Systems

☐ Inspect.

☐ Test.

☐ Eliminate weaknesses.

☐ Maintain record of all alarms: include date, time, location, action taken and cause.

☐ Maintain record of response time on service calls.

☐ Provide for automatic emergency power supply; secure.

☐ Require scheduled maintenance.

☐ Require identification of maintenance/service personnel; record date, times, station identification, and name of person.

☐ If proprietary system, provide security for control station.

☐ Require that console be manned at all times.

☐ Test to insure that annunciators on console readily identify sector covered.

☐ Provide fail-safe and tamper provisions.

☐ Conduct frequent tests to determine adequacy and promptness of response to alarm signals.

Guards

☐ Prescribe qualifications.

☐ Screen before hiring.

☐ Train and test.

☐ Uniform.

☐ Arm, if authorized and necessary.

☐ Equip; provide for replacement equipment.

☐ Commission as special police or deputy, if appropriate.

☐ Explain authority of guard.

☐ Provide communications.

☐ Plan for sickness; absence.

☐ Publish brief, clear orders: general and special.

☐ Provide for timely revision of published orders; avoid practice of penciled or pen and ink changes.

☐ Brief each relief.

☐ Patrol via irregular route on random schedule.

☐ Require log of activities for each relief.

☐ Require incident report for each unusual incident or irregularity.

☐ Provide for emergency assistance.

☐ Supervise; supplement with artificial systems.

☐ Provide for 24-hour heating/cooling in control center.

☐ Provide locker room and secure equipment stowage.

☐ Give refresher training.

PART V IDENTIFICATION AND MOVEMENT CONTROL

PERSONNEL CONTROL

Employees

☐ Screen applicants to eliminate potential risks.

☐ Train all employees in security measures and evacuation procedures.

☐ Require personnel recognition; up to 30 persons.

☐ Use single pass or badge system.

☐ Use single pass or badge system, coded by a color, letter, or number, to designate area, plant, or department for which valid.

☐ Use pass/badge exchange system.

☐ Use electronic identification system.

☐ Provide controls for badge stocks.

☐ Provide guards with sample badges, preferably framed.

☐ Insure return and destruction of badges, on termination of personnel.

☐ Require written report from person who loses pass or badge.

☐ Provide guards list of lost or stolen badges.

☐ Prescribe method for wearing badge.

☐ Prescribe method for handling, e.g., hand badge to guard.

Visitors

☐ Designate visitors' entrance.

☐ Verify visit by telephone.

☐ Require sign-in/sign-out by visitors.

☐ Issue visitor's pass.

☐ Provide positive means of recovering visitor's pass.

☐ Use color-coded, data-stamped, one day throw-away visitor's pass.

☐ Require validation of pass by person visited.

☐ Use timed travel visitor control system.

☐ Obtain escort from office being visited.

☐ Use escort pool.

☐ Restrict areas to visitors; post with signs.

☐ Require escort for designated areas.

☐ Use access list.

Vehicle Control

☐ Prohibit unauthorized vehicles.

☐ Verify that service trucks and other such vehicles require access.

☐ Require driver's identification.

☐ Require sign-in by driver.

☐ Require list of drivers, and description of vehicles which may require access.

☐ Provide guard with description and license of organizational vehicles; require verification and examination of personnel identification before permitting into area.

☐ Maintain log of all vehicles which enter/leave area.

☐ Identify critical areas; install physical barriers to prevent vehicle access to these areas.

☐ Inspect vehicles prior to entering area.

☐ Inform guards of pattern of activity of commercial vehicles; post diagram in control center.

☐ Provide escort for each vehicle.

☐ Require vehicles to park outside gate; provide shuttle service.

INDEX

END