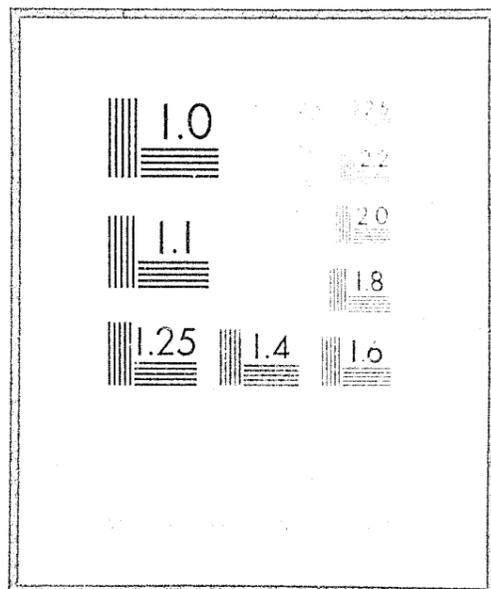


NCJRS

This microfiche was produced from documents received for inclusion in the NCJRS data base. Since NCJRS cannot exercise control over the physical condition of the documents submitted, the individual frame quality will vary. The resolution chart on this frame may be used to evaluate the document quality.



Microfilming procedures used to create this fiche comply with the standards set forth in 41CFR 101-11.504

Points of view or opinions stated in this document are those of the author(s) and do not represent the official position or policies of the U.S. Department of Justice.

U.S. DEPARTMENT OF JUSTICE
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
NATIONAL CRIMINAL JUSTICE REFERENCE SERVICE
WASHINGTON, D.C. 20531

1/13/77

36482 6.5

Prevention of Terroristic Crimes: Security Guidelines for Business, Industry, and Other Organizations

LOAN DOCUMENT
RETURN TO:
NCJRS
P. O. BOX 24036 S. W. POST OFFICE
WASHINGTON, D.C. 20024

A REPORT PREPARED BY THE
PRIVATE SECURITY ADVISORY COUNCIL,
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION,
U.S. DEPARTMENT OF JUSTICE

36482 6.5

LAW ENFORCEMENT ASSISTANCE ADMINISTRATION

RICHARD W. VELDE, ADMINISTRATOR

PRIVATE SECURITY ADVISORY COUNCIL

CHAIRMAN

Arthur J. Bilek

VICE CHAIRMAN

Howard L. Mai

FEDERAL REPRESENTATIVE

Irving Slott

MEMBERS

Saul Arrington

Jim L. Bridges

Walter Burns

Richard C. Clement

Richard F. Cross

Jackie Currie

Joseph F. Doherty

James W. Ferriman

Eugene L. Fuss

Harold W. Gray, Jr.

Edward W. Hyde

David B. Kelly

Fritz A. Schumacher

Geoffrey C. Shepard

Howard C. Shook

George A. Smith, Jr.

John L. Swartz

C. W. Thompson

James H. Young

PREVENTION OF TERRORISTIC CRIMES:

SECURITY GUIDELINES

FOR

BUSINESS, INDUSTRY AND OTHER ORGANIZATIONS

Prepared By The:

PRIVATE SECURITY ADVISORY COUNCIL
TO THE
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
U.S. DEPARTMENT OF JUSTICE

MAY 1976

Points of view or opinions expressed in this document are those of the Private Security Advisory Council, and do not necessarily represent the official position or policies of the Law Enforcement Assistance Administration, U.S. Department of Justice.

**PRIVATE
SECURITY ADVISORY COUNCIL of the**

United States Department of Justice
Law Enforcement Assistance Administration

May 14, 1976

Mr. Richard W. Velde
Administrator
Law Enforcement Assistance Administration
U.S. Department of Justice
633 Indiana Avenue, N.W.
Washington, D.C. 20531

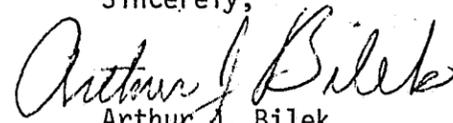
Dear Mr. Velde:

As Chairman of the Private Security Advisory Council, it gives me pleasure to forward the attached document, Prevention of Terroristic Crimes: Security Guidelines for Business, Industry and Other Organizations, developed by the Council for the Law Enforcement Assistance Administration. This document is the culmination of many hours of volunteer effort by members of the Private Security Advisory Council and the members of the Prevention of Terroristic Crimes Committee of the Council. With the alarming increase in terroristic attacks against corporate enterprises as well as other organizations, the Council and the Prevention of Terroristic Crimes Committee felt an urgent need to develop basic security guidelines against this type of crime.

The Advisory Council firmly believes that these security guidelines will be useful to business executives, government officials, and private security specialists in developing preventive measures against various types of terroristic threats and acts. Further, the Advisory Council recommends that the Law Enforcement Assistance Administration give the widest possible dissemination to this document.

With best personal regards,

Sincerely,



Arthur J. Bilek
Chairman
Private Security Advisory Council

AJB:aml

Enclosure

TABLE OF CONTENTS

PREFACE.....	i
THE PRIVATE SECURITY ADVISORY COUNCIL.....	ii
INTRODUCTION.....	1
DEFINITION OF TERRORISM.....	3
SECURITY RESPONSIBILITY.....	5
LAW ENFORCEMENT LIAISON.....	6
OFFICE AREA PROTECTION.....	7
1. Office Accessibility.....	7
2. Alarm Protection.....	7
3. Visitor Controls.....	8
4. After Hours Access.....	8
5. Executive Office Area Restrooms.....	8
6. Maintenance Closets.....	9
7. Telephone and Electrical Equipment Rooms.....	9
8. Executive Office Area Key Controls.....	9
9. I.D. Badges.....	9
10. Fire Protection.....	10
11. Safe Room.....	10
12. Emergency Supplies.....	10
13. Publicity Releases.....	10
14. Incoming Mail.....	10
15. Parking.....	11
16. Travel Plans.....	11
PERSONAL PROTECTION FOR THE EXECUTIVE.....	12
1. Low Executive Profile.....	12
2. Avoid Routines.....	12



PERSONAL PROTECTION FOR THE EXECUTIVE (cont'd)

- 3. Recognition of Surveillance..... 12
- 4. Travel Arrangements..... 12
- 5. Code Systems..... 12

RESIDENTIAL AND FAMILY PROTECTION..... 13

- 1. Family Awareness..... 13
- 2. Pretexts or Ruses..... 13
- 3. Physical Protective Measures..... 13
 - A. Door Viewing..... 14
 - B. Door Locks..... 14
 - C. Windows..... 14
 - D. Lighting..... 15
 - E. Alarms..... 15
 - F. Safe Room..... 15
- 4. Unlisted Telephone Numbers..... 16
- 5. Suspicious Activities or Occurrences..... 16
- 6. Emergency Plans..... 16
- 7. Travel Plans..... 17

PROTECTION WHILE TRAVELING..... 18

- 1. Automobile Travel..... 18
- 2. Aircraft Travel..... 18
 - A. Commercial Aircraft..... 18
 - B. Company Aircraft..... 19

KIDNAPPING..... 20

- 1. Emergency Biographical Data Sheets..... 20

KIDNAPPING (cont'd)

- 2. FBI Guidelines..... 21
 - A. Safeguards for Children..... 21
 - B. Kidnapping Involving Ransom..... 23

EXTORTION THREATS..... 25

- 1. Telephone Threats..... 25
 - A. Notification Form..... 25
 - B. Actions During The Call..... 27
 - C. Actions After The Call..... 28

ASSESSING ORGANIZATIONAL TARGETS..... 29

PREFACE

This document, Prevention of Terroristic Crimes - Security Guidelines for Business, Industry and Other Organizations, was developed by the Private Security Advisory Council and its Prevention of Terroristic Crimes Committee in response to a critical need to alert executives and other concerned groups to the potential threats posed by terrorists, and to present various techniques and precautions that should be employed to prevent these types of violent acts. In America, as in other countries throughout the world, terrorist attacks have increased dramatically during the past few years. Therefore, it is essential that possible targets (organizations and individuals) understand this exceptional type of crime and take precautions to minimize the risk of becoming victims to the terroristic act.

The brief guidelines contained in this document are not by any means all-inclusive; the Prevention of Terroristic Crimes Committee to the Council is currently preparing a requirements document for a detailed countermeasures manual against various forms of terroristic crimes. These guidelines are intended to provide an awareness of basic measures to prevent terroristic crime and to cope with threats from suspected terrorists.

The major effort in developing this document was performed by the Prevention of Terroristic Crimes Committee, and special acknowledgement and appreciation is due the Chairman and members of that Committee: Albert Davis (Chairman), Joseph Blank, Ernest H. Dunham, John M. Kirsch, E. M. Lembke, Rocky Pomerance, Kenneth Porter, and Fred Rayne.

The Prevention of Terroristic Crimes Committee was assisted in preparing this document by members of the Council's staff support contractors: PRC Public Management Services, Inc., and Hallcrest Systems, Inc., specifically Consultant Jan Reber.

The Advisory Council owes a special debt of gratitude to Irving Slott, Federal Program Monitor to the Council, for his encouragement and counsel in the development of this document.

Arthur J. Bilek
Chairman
Private Security Advisory Council

THE PRIVATE SECURITY ADVISORY COUNCIL

The Private Security Advisory Council was chartered by the Law Enforcement Assistance Administration (LEAA) in 1972 to improve the crime prevention capabilities of private security and reduce crime in public and private places by reviewing the relationship between private security systems and public law enforcement agencies, and by developing programs and policies regarding private protection services that are appropriate and consistent with the public interest.

The Council was an outgrowth of a meeting of private security sector representatives, called by LEAA in December 1971, to discuss the research and development efforts of LEAA that related to the private sector and the role of private security in the national effort to reduce crime. During the initial meeting, representatives from the private security sector overwhelmingly recommended that LEAA establish a national advisory committee, made up of persons with expertise in private security, to provide LEAA with continuing advice on matters of appropriate concern. LEAA followed that recommendation, and the Private Security Advisory Council was created shortly thereafter.

In September of 1974, the membership of the Council was broadened to include representation from the public law enforcement agencies and from consumers of private security services. Since its inception, the Council has worked on a number of tasks related to security services provided by the private sector. As established in 1974, the goals and objectives of the Council were:

- To act as an advisory to LEAA on issues of national importance which impact, or are impacted by, the private security industry;

- To raise the standards and increase the efficiency of the private security industry;
- To increase cooperation and understanding between the private security industry and public law enforcement; and
- To provide a viable national forum and point of leadership for matters relating to private security.

To achieve those goals, the Council established five committees: Alarm Committee, Environmental Security Committee, Guards and Investigators Committee, Law Enforcement/Private Security Relationships Committee, and the Prevention of Terroristic Crimes Committee. Each committee was assigned specific objectives related to accomplishment of Council goals.

The responsibilities and duties of the Private Security Advisory Council are advisory in nature. It cannot prescribe or promulgate rules or regulations. Its findings or recommendations are not official; they can be accepted or rejected by LEAA.

The Council operates pursuant to the provisions of the Federal Advisory Committee Standards Act, Public Law 92-463, LEAA Notice NI300.2, OMB Circular No. A-63, and any additional orders and directives issued in implementation of the Act. The Council was established under the authority of Section 517 of the Omnibus Crime Control and Safe Streets Act of 1968 (Public Law 90-351) as amended by Public Law 91-644 and the scope of its functions is limited to the duties specified in its charter.

The Council has published a number of other advisories to LEAA on a variety of issues. These include:

- A Report on a Model Hold-Up and Burglar Alarm Business Licensing and Regulatory Statute;

INTRODUCTION

- A Report on the Regulation of Private Security Guard Services, including a Model Private Security Licensing and Regulatory Statute;
- Terroristic Crimes: An Annotated Bibliography;
- Potential Secondary Impacts of the Crime Prevention Through Environmental Design Concept;
- Reports on the Private Security Advisory Council Meetings of June 1974, September 1974, February 1975, July 1975, October 1975, and November 1975.

In addition to the above reports, the Private Security Advisory Council and its Committees, are preparing other advisory reports to LEAA on the need for and requirements of, a national study of the false alarm problem; the scope of legal authority of private security personnel; codes of ethics for private security management and private security employees; areas of conflict between private security and public law enforcement; the requirements of a comprehensive manual on countermeasures against terroristic crimes; standards for private investigators; and crime impact statements as an environmental security technique.

Terrorism often appears to be unpredictable and even irrational to its victims, but terrorists are usually rational individuals who use terror tactics to achieve finite goals. Most terrorists believe that their actions will eventually disable business and government and will increase their popular support so that they can achieve their goals. Today's terrorists are media-sophisticated; they are aware that violence brings publicity. Further, the terrorist underground operates in "hard-to-infiltrate" small groups, rendering public law enforcement less capable of thwarting their activities.

From 1973 to 1974, bombings in this country have risen 50 percent, and deaths from such incidents have increased twelve-fold. In California alone bombings are occurring three times faster than a year before. Law enforcement and security experts expect this trend to increase throughout this bicentennial year.

With an expected increase in terrorist violence against the perceived "power" structures in this country (government and industry) and the concomitant inability of public law enforcement to stem this tide, it becomes imperative that those in the private security sector take cognizance of the possibility of future violence and prepare themselves and their organizations to act as the first barrier against terroristic crimes.

Since the most serious terrorist attacks are those directed toward the individual, the preventive measures outlined in this guide are primarily oriented toward the safety of the individual and his family while at work, at home and during travel. These measures are intended to help minimize the risk of such attacks by providing a "before-the-fact" awareness of those preventive actions which can be taken to reduce or deter such attacks. Such preparedness is essential if effective security countermeasures are to be realized. While American law enforcement agencies are doing their utmost to combat this serious type of crime,

those persons who may be targets of terroristic attacks must be alert to this real and potential problem.

As indicated in the text, additional information pertaining to terrorist security countermeasures may be available from security managers within business organizations as well as from local, state, and federal law enforcement agencies.

DEFINITION OF TERRORISM

There are varying definitions of terrorism which is due in part to the fact that acts of terrorism are perceived differently by the victim, the perpetrator, and by others who are not directly involved as victims or perpetrators.

The Private Security Advisory Council's Committee on the Prevention of Terroristic Crimes has defined terrorism as "criminal acts and/or threats by individuals or groups designed to achieve political or economic objectives by fear, intimidation, coercion or violence." Such acts as kidnapping, bombing, sabotage, assassination, extortion or other terroristic acts, whether politically or criminally motivated, are of concern to this Committee.

Terrorism for political purposes may be employed to publicize the existence of a particular group with a particular set of grievances, but it is usually employed to persuade the population and the government that specific political and social changes must occur.

There are at least nine characteristics that are common to the vast majority of terrorist acts:

1. The use of violence as a method of systematic persuasion;
2. The selection of targets and victims with maximum propaganda value;
3. The use of unprovoked attacks;
4. The selection of acts that gain maximum publicity with minimum risk to the terrorist;
5. The use of surprise to overcome countermeasures;
6. The use of threats, harassment, and violence to create an atmosphere of fear;
7. The lack of recognition of civilians or women and children as "noncombatants;"

8. The use of propaganda to maximize the effect of violence and to achieve political or economic goals;
9. The perpetration of terroristic acts by groups whose only loyalty is to each other.

SECURITY RESPONSIBILITY

It is recommended that a responsible member of management be assigned the primary responsibility for instituting security measures in an organization. Depending upon the size and scope of the organization, this individual should devote most, or all, of his endeavors to the formulation of preventive security measures which include personnel awareness programs and promulgation of security countermeasures to minimize the number of terroristic incidents and their effects. Most organizations within the U.S. today have an individual with security responsibility. In many instances, this security specialist is responsible for the development of comprehensive security programs for both personnel and assets protection. The degree of expertise and level of specialization required to cope with today's security problems is such that utilization of a security professional is a sound business practice.

The overall security measures enforced by organizations help to minimize the likelihood of terrorist actions. For instance, such general considerations as personnel security screening, positive employee identification, and tight perimeter access control are essential. These programs should include positive visitor identification, and badging with restricted area escorting as well. Likewise, specific identification measures and controls for vendors, service people, and other nonemployees who have intermittent or regular access to a facility should not be overlooked.

The overall physical protective level of a facility should also be evaluated: regular reviews should be made to ensure the adequacy of lock and key systems, of fencing and lighting equipment, and of supplemental intrusion alarm protection for sensitive areas. Other protective techniques utilizing surveillance systems such as closed circuit television may also be required to assure minimum security protective levels in any organization. The security specialist should conduct a comprehensive vulnerability assessment to determine the adequacy of the physical protective measures and the general security posture of the facilities.

LAW ENFORCEMENT LIAISON

In the formulation of any plan to minimize the possibility of terroristic acts, liaison with law enforcement agencies is essential. Should a threat or actual physical attack be made by terrorists, the immediate assistance of a law enforcement agency will be required.

Organizations should establish and maintain close personal working relationships with representatives of law enforcement agencies in their immediate areas. Contingency plans should be specified and then reviewed and updated periodically. Procedures for notifying law enforcement agencies in the event of a kidnapping, bombing or other terroristic threat or act must be clearly defined beforehand and incorporated into the organization's overall security countermeasures plan.

Law enforcement officials should be supplied with the names, addresses, home telephone numbers and area of responsibility of all organization officials who have the authority to confer with law enforcement agencies and make policy decisions during crises. In addition, information that law enforcement officials may require during a crisis, such as photographs and home telephone numbers of kidnapped executives, layouts of buildings which may contain a bomb, etc., should be readily available for their use.

OFFICE AREA PROTECTION

Countermeasures against terrorism can and should be implemented in the corporate environment. Terrorists have selected offices as targets for bombings, sabotage, demonstrations, abductions, and murders. The following list describes some of the measures which may be useful in deterring such terroristic acts.

1. Office Accessibility

Depending upon the type of business and the specific location of the office area within the facility, those offices most likely to be targets of terrorism should not be directly accessible to the public. Executive office areas should not be located on ground floor levels. If office windows face public areas, they should be curtained and reinforced with bullet resistant materials. The direct and immediate access to executive offices should be monitored by a secretary, guard or other individual who screens all persons and objects entering executive offices.

The most effective physical security configuration is to have doors locked "from within," with one visitor access door for ingress to the executive office area. Locked doors should have panic bars and local annunciation. The ingress door should be within the view of the person(s) responsible for screening personnel and objects which will pass through the door. The door may be remotely controlled by installing an electro magnetic door lock for use by a secretary, receptionist, guard, or by the executive himself.

Depending upon the nature of the organization's activities, it may be best to draw attention away from the location and function of the office.

2. Alarm Protection

The point at which visitors enter executive offices should be equipped with a hidden and unobtrusive means of activating an emergency alarm.

This alarm can sound at an organization's security or guard center, at the executive's desk, or at any other location where a signal would summon immediate assistance. The executive's desk should also be equipped with a hidden alarm-activation device to enable him to signal for aid should an intruder gain entrance to his office.

3. Visitor Controls

Controlled and escorted visitor access into executive office areas is an essential element of an organization's security policies. Any unescorted visitor or unidentified person noticed in that area should be promptly challenged. Where there is overall perimeter visitor screening, all visitors to executive office areas should be required to show positive identification; this information should be logged and an identifying badge given to visitors before they are escorted to the executive offices.

In high risk areas, a metal detector may be used to screen packages and other objects being carried into the executive area.

4. After Hours Access

A very careful examination must be made of the measures for controlling the admittance of all persons into the executive area during nonworking hours. These measures may specify that all cleaning and maintenance personnel will be escorted by a guard or supervisor, as well any other persons requiring nonworking hours access into such areas. In addition, guards should be directed to make periodic checks of executive office areas in their after-hours tours.

5. Executive Office Area Restrooms

All restrooms on the floors where executive offices are located (as well as others in a multistory office building) should be locked to eliminate unrestricted public access. If the executive offices are situated in a

building which is accessible to the public, the probability of bombs being hidden in these areas, or intruders hiding in them, is greatly increased. Locking such rooms provides added protection for female personnel against robbery and personal attacks.

6. Maintenance Closets

Doors to janitorial and other maintenance closets should be kept locked at all times. Specific key issuance and accountability controls with key issuance limited to supervisory janitory personnel is recommended.

7. Telephone and Electrical Equipment Rooms

Doors to telephone and electrical equipment rooms should be kept locked and access given to maintenance and telephone personnel who have a requirement for such access.

8. Executive Office Area Key Controls

Stringent lock and key control measures pertaining to immediate executive office areas, desks, and office files are of paramount importance. Wherever possible, door locks and keys should not be on the same master key control system as the rest of the facility. A separate locking system, preferably utilizing changeable cores which are periodically rotated with systematic key accountability audit controls, is desirable.

9. I.D. Badges

The use of I.D. badges with a photograph of the bearer and a handwriting sample of signature as well as other identifying data is advised. Automated card readers or push-button door locks may be employed to allow entry to authorized persons. In high risk situations, it may be advisable for all personnel to wear their I.D. badges while on the premises.

10. Fire Protection

The facility should have fire detection and a fire suppressant capability. Extinguisher should be readily available as a minimum safeguard.

11. Safe Room

An interior safe room for use by likely targets in the event of a terrorist attack should be considered. It should not be easily accessible from the outside, should have a sturdy door and lock, and should not be identifiable as a safe room. Emergency, first aid, and communicating equipment should be kept there.

12. Emergency Supplies

Emergency supplies such as first aid equipment, bomb blankets, candles, food rations, lanterns, communications equipment, portable radios and other appropriate equipment should be maintained at the facility, and key personnel should know their locations as well as the location of emergency exits and escape routes.

13. Publicity Releases

Companies should maintain as confidential personal history data regarding high-level executives since this may be useful to terrorists in selecting victims or in identifying their homes and families.

14. Incoming Mail

Security awareness measures relating to the screening of incoming mail (and packages) for executive personnel should be in effect. While it is not possible here to list all of the preventive measures which can be taken to screen executive mail, procedures for identifying and checking suspicious letters and packages must be considered. Equipment is commercially available for checking the contents of suspicious letters and packages.

As a minimum, mailroom supervisors should inspect executive mail for suspicious envelopes and packages. As a second line of defense, executive secretarial personnel should be alerted to check for suspicious letters and packages delivered to them.

Other equipment, such as bomb blankets and steel containers for temporary storage of suspicious mail should be considered.

It is also recommended that each facility ascertain the identity and location of the nearest bomb handling and disposal unit. This may be either a local, state or federal law enforcement agency or a U.S. Department of Defense military facility.

15. Parking

It is recommended that executive personnel areas not be conspicuously identified as such, and that parking spaces be identified by number rather than by the names of individual executives.

16. Travel Plans

Information on travel itineraries and arrangements should not be publicized, but restricted to as few persons as possible. Written agenda and other correspondence regarding such plans should be tightly controlled and safeguarded in the same manner as other sensitive company information.

PERSONAL PROTECTION FOR THE EXECUTIVE

1. Low Executive Profile

The effectiveness of executive protective measures is heavily dependent upon the executive's ability and willingness to maintain a low profile. In this connection, publicity regarding the executive should be kept to a minimum in advertising campaigns, publicity releases, and social columns. This is especially true with respect to photographs of key executives and personal information regarding families, personal affairs (including incomes), travel plans, club memberships, and social activities.

2. Avoid Routines

Executive personnel should avoid regular patterns which are easily discernible. Arrival and departure times as well as routes taken to and from work should be varied as often as possible. The routes of travel should be along well populated and lighted public roadways.

3. Recognition of Surveillance

Executives should be taught to recognize signs which may indicate that they are under surveillance by strangers.

4. Travel Arrangements

Executives should always advise a family or organizational member of their destination and expected time of arrival when traveling. In a high-risk situation these precautions should be taken daily when leaving for or from the office.

5. Code Systems

Simple, effective, verbal code signals for alerting family and organizational members of danger should be individually established for each executive.

RESIDENTIAL AND FAMILY PROTECTION

One of the most difficult places to institute security measures is the residence. Homes are rarely built with security in mind, and can generally be penetrated with relative ease. Certain practical preventive measures, though, are applicable to the residence and the family living in it. Individual security surveys of private residences will indicate how best to upgrade the level of protection at the residence.

Some general areas of consideration for residential and family security follow:

1. Family Awareness

Residential and family security measures can only be effective if all household members have developed security awareness. The objective should not be to instill fear or apprehension, but to make the family alert to suspicious activities or occurrences. Terrorists prey on the weakness of unsuspecting victims, and only security awareness can counter this threat.

2. Pretexts or Ruses

All family members should adopt a questioning attitude toward persons seeking entry to the residence. Admittance should not be granted unless the family member is completely satisfied as to the identity and purpose of the caller. Visits by repairmen, utility company representatives, salespersons, government inspectors, etc., should be based on prior arrangements with the organization involved. In high-risk situations, a call to the organization to verify the identity of the visitor is advisable.

Pretexts by "distressed motorists" or others to gain access to the residence for emergency reasons (such as telephone use) should be guarded against. Should such a situation occur, it is best to have the person remain outside with the door locked, while you make an emergency telephone call for assistance on their behalf.

Many pretexts are made by telephone. Any inquiries about the whereabouts or activities of family members should be treated with suspicion.

3. Physical Protective Measures

Most residences offer little physical protection against a terrorist. However, there are certain physical protective techniques which should be considered to reduce this vulnerability.

A. Door Viewing

Front and back doors should be provided with a means of observing the caller from within. There are, of course, products available for installation in solid doors for outside viewing purposes.

B. Door Locks

Supplemental chain-bolt locks should be used wherever practical to permit doors to be opened slightly but still in a secured position.

Double dead-bolt door locks should be considered for front and back doors which require positive keying on both sides to open. Basement and/or garage access doors, as well as fuse boxes in such locations should be padlocked. Glass doors should have special locks to prevent the prying open of the doors.

C. Windows

In high-risk situations, shutters or smash-resistant materials should be used to increase window protection.

D. Lighting

Protective lighting for deterrent purposes should be used inside and for the immediate surrounding area of the home. Outside lighting should illuminate the area surrounding the dwelling and access driveway to the residence. Such lighting can be installed to be activated manually, by automatic light sensing devices, or by intrusion alarm systems.

Electric timers for various rooms and hallways within the dwelling can also be utilized. Such timers can also be used with radios and televisions to give the appearance that the residence is occupied. Random timers which turn lights and other devices on and off at predetermined times increase the "lived-in" appearance of a residence.

E. Alarms

The use of an electronic alarm system should be considered. "Local alarms" provide a loud, audible signal when protected areas such as doors and windows are tampered with. Other types of alarm systems (silent) may be wired into local police departments or to commercial alarm companies. The alarm system may also contain fire detection devices and provide a distinctly audible signal when fire is detected. The purpose of an intrusion alarm system is to deter and detect unauthorized tampering and entry into the residence, and it serves only as a warning, not as a defense against the intrusion.

F. Safe Room

An interior room of the residence may be prepared for use as a safe haven during a terrorist attack. It should be unobtrusive and should have a sturdy, solid door, a heavy lock and

hinges, and an emergency exit, if possible. The room should contain a communications device such as a radio or telephone as well as emergency supplies.

The preparation of a safe room does not negate the need for escape plans to be used during a fire or other emergency. The safe room is exclusively for use during a terrorist attack which can not be avoided by escape.

4. Unlisted Telephone Numbers

For obvious reasons it is recommended that key executives have their home telephone numbers unlisted. Additional telephone number and home address information safeguards should also be considered to minimize access to such information by any unauthorized individuals. Family members should not identify themselves when answering the telephone until they have identified the caller.

5. Suspicious Activities or Occurrences

Family members should be alert to suspicious occurrences, for example, strangers who are repeatedly seen in or about the residence. Their presence should be noted and a record made of any vehicles they drive; descriptions should be obtained of such strangers where possible. Suspicious persons should be reported to the local law enforcement agency.

6. Emergency Plans

All family members should be familiar with emergency telephone numbers and when to use them. Special procedures to be followed in the event of an emergency should also be familiar to all family members. These include the use of codes to signal distress, and the implementation of evacuation plans.

7. Travel Plans

It is advisable that information regarding travel plans be kept confidential. The decision to stop mail and news paper delivery, the cancellation of regular appointments such as hairdressers, recreational and social activities, etc. should be carefully evaluated to determine whether the stoppage is really necessary and might alert potential attackers and whether more discreet means should be used to arrange required stoppages.

PROTECTION WHILE TRAVELING

Since personnel are very vulnerable while traveling regular routes to and from places of business and other locations regularly visited, frequent changes of routes, times, and days are desirable. Wherever possible, executives should avoid traveling alone at late hours on a regular basis.

1. Automobile Travel

It is generally recommended that doors be kept locked and windows closed during automobile travel. When not in use, vehicles should be kept in a locked garage or other areas not readily accessible. Locking of gas tank caps is also recommended, and gas tanks should never be less than half full. Automobile intrusion alarm systems as well as two-way radio or telephone communication in vehicles is desirable.

There are specific avoidance tactics regarding vehicle ambush attacks. Specific information and training techniques regarding such defensive measures should be obtained from security specialists or law enforcement agencies.

If chauffeurs or other individuals are used for drivers on a regular basis, they should receive formal instruction in offensive and defensive driving techniques so that they will be able to recognize and avoid terrorist ambushes and other forms of attack.

2. Aircraft Travel

A. Commercial Aircraft

Travel on commercial airlines has now become one of the most secure means of travel in the United States. Ground security protective measures and other anti-hijack techniques have made commercial airlines a most desirable means of travel for executive personnel.

The kidnapping threat is now considered less of a risk factor in air travel than in other means of travel. However, individuals should be mindful that in most overseas locations, ground security measures are not generally as effective as those within the United States.

B. Company Aircraft

Unless specific preventive measures have been taken, there is a higher risk factor in traveling by company aircraft than by commercial aircraft. Physical protective safeguards for the private aircraft and hangar, access controls, etc. are not as formidable to the terrorist as they are at protected commercial airfields. However, locked hangars, cabins, and access ports, as well as utilization of aircraft intrusion and tamper alarm systems can be considered. Protective measures to limit direct access to aircraft are essential. Preflight security inspection measures and preboarding, "all-clear" procedures by the pilot and crew should be instituted. The feasibility of guard utilization at high-risk locations must also be evaluated.

Another aspect of air travel to consider is the travel to and from an airfield. Fields used for private aircraft may well be located in rural or unpopulated areas accessible only by infrequently traveled roads. Security measures for vehicular travel as previously discussed should be considered.

Security specialists should be consulted for more specific guidelines regarding aircraft protection measures. It is important that the aircraft be protected while at other airfields and that the plane have no distinctive organizational markings.

KIDNAPPING

1. Emergency Biographical Data Sheets

In the event that a kidnapping should occur, it is very important that a complete record of personal information be immediately available for law enforcement investigative use. It is recommended that complete biographical data regarding key executive personnel be maintained in one central location, perhaps in the files of the organization's security manager. Access to this information should be highly restricted, and positive storage controls, such as storage in three-position combination locked files, are recommended. The data should only be used for emergency purposes. Such information should include color photographs of the individuals (as well as the family), fingerprints, signature samples and voice tapes. The information should be kept in individual envelopes sealed by the executive and updated by him on a regular basis.

The biographical data included in the file should, as a minimum, include:

- Complete name(s);
- Addresses of primary and secondary residence, as applicable;
- Personal telephone numbers;
- Complete physical descriptions: distinguishing physical features such as scars or other identifying and unique physical characteristics;
- Banks where money may be deposited and where withdrawals may be made;
- Name of local physician, dentist, optician;
- Family cars driven: state license numbers, make, model, year and color, and vehicle identification numbers;
- Schools attended by children;
- Names, addresses and telephone numbers of immediate family or other relatives who could be contacted regarding whereabouts of the family;
- Credit card companies and card numbers;

- List of boats, campers, or other recreational vehicles;
- Profile of hobbies, clubs, and other activities in which family members participate.

2. FBI Guidelines

Should a kidnapping attempt be made or an actual kidnapping occur, the security guidelines issued by the FBI in 1974 should be followed. These protective security measures are as follows:

A. Safeguards for Children

1. Keep the door to the children's room open so that any unusual noises may be heard.
2. Be certain that the child's room is not easily accessible from the outside.
3. Never leave young children at home alone or unattended and be certain that they are left in the care of a responsible, trustworthy person.
4. Instruct the children to keep the doors and windows locked and never to admit strangers.
5. Teach the children, as early as possible, how to call the police; and instruct them to contact the police if strangers or prowlers are seen around the house or attempt to get in.
6. Keep the house well lighted if it is necessary to leave the children at home.
7. Instruct servants not to let strangers in the house.

8. Make arrangements with schools attended that before releasing a child to anyone, other than their parents, during the regular school day, a teacher or administrative official should telephone a parent or guardian for approval.

In this connection, when a parent telephones a request that a child be released early from school, the identity of the caller should be confirmed before the child is permitted to leave. If the parent is calling from his home, the school should be advised to verify the request by a return telephone call, during which the child should identify the parent's voice. In the event the telephone call is not being made from the child's residence, the caller should be asked a few questions about the child which should be known only to the parents. Such questions, or other identifying arrangements such as a code phrase, could include the child's date of birth, the courses he is studying, names of his teachers and classmates, and so forth. Where there is any doubt, the school should be instructed not to release the child.

9. Schools, as well as parents and youth agencies, should take steps to make sure that adult supervision is provided in school and recreation areas.
10. Advise children to:
 - a. Travel in groups or pairs:
 - b. Walk along heavily traveled streets and avoid isolated areas, where possible;
 - c. Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot;

- d. Use city-approved play areas where recreational activities are supervised by responsible adults and where police protection is readily available;
- e. Immediately report anyone who molests or annoys them to the nearest person of authority;
- f. Never leave home without telling their parents where they will be and who will accompany them.

B. Kidnapping Involving Ransom

Whenever a kidnapping occurs, it is essential that the victim's family immediately initiate action to effect the safe return of the victim. This can best be accomplished if the family of the victim carries out the following recommendations:

1. Telephone the Federal Bureau of Investigation. The telephone number of the nearest FBI office is listed in the front of every telephone directory; the emergency telephone number at FBI Headquarters in Washington is Area Code (202) 324-3000. The complainant should be prepared to furnish all facts relating to the disappearance of the victim.
2. Maintain absolute secrecy and do not reveal any of the facts regarding the kidnapping or demands for ransom to anyone outside the immediate family except the appropriate law enforcement authorities and the organization's security manager.
3. Do not handle letters or communications demanding the payment of ransom. Turn these over to the law enforcement agency handling the matter as soon as possible.

4. Neither touch nor disturb anything at the scene of the crime. Minute particles of evidence which are invisible to the naked eye may be destroyed.
5. Be calm and strive to maintain a normal routine around the home and office as much as possible.
6. Place full confidence in the law enforcement officers who are investigating the kidnapping. In addition to photographs and a complete description of the victim, it is essential that law enforcement officers be provided with all facts relating to the personal habits, characteristics and idiosyncrasies of the victim. Utilize the Emergency Biographical Data Sheet for this purpose.

EXTORTION THREATS

1. Telephone Threats

Since most extortion threats are received by telephone, certain preventive security measures should be established to handle them. One of the most important measures is to equip a telephone with a recording device to tape the conversation which transpires, should such a call be received. Copies of actual conversations can be of significant value for subsequent voice-print investigative purposes, as well as for recall of instructional details which may be discussed. Federal law requires that at least one party to a conversation be aware that the call is being recorded. Individual states have various requirements for "beep tones" during recordings.

A. Notification Form

Additionally, a means should be established to quietly notify a secretary or someone else in close proximity that an extortion call is being received. A preprinted extortion readiness form is most commonly used for this purpose. The preprinted form should include the following pertinent information filled in beforehand:

1. I have received a telephone threat on line:

a. _____

b. _____

c. _____

At _____ o'clock

2. Please notify the telephone company (telephone number: _____) of the threat and request an immediate line trace.

3. The caller states that he/she has kidnapped:

- a. _____
- b. _____
- c. _____
- d. _____

4. The caller has made the following specific threats:

5. Call my home number at _____
and try to verify the whereabouts of:

- a. _____
- b. _____
- c. _____
- d. _____

6. Call the local -

- a. FBI Office -
Telephone Number _____
- b. Police Department -
Telephone Number _____
- c. Security Manager -
Telephone Number _____
- d. Other _____

B. Actions During The Call

During the call itself, it is important to:

1. Stay calm.
2. Try to verify that the caller has the hostage or that the threat is real. This may be done by requesting to speak to the victim or by asking questions regarding personal details known only to the victim.
3. Although the tactic will be well known to the caller, try to keep the caller on the telephone as long as possible. This means the person receiving the call will have to be a good listener, but must also be able to prolong the conversation. As previously stated, this will require calmness on the part of the person receiving the call as well as an awareness of what questions to ask the caller. It is important to gain the caller's confidence so that he will reveal as many specifics about the incident as possible.

4. In all cases express complete cooperation with the caller and do nothing to antagonize or terminate the call.
5. Communicate to the caller the problems of immediate compliance with his demands, especially those related to ransom.

C. Actions After The Call

Immediately after an extortion call is received, do the following:

1. Make sure the FBI or local law enforcement officials and the organization's security manager are immediately notified. Such notification is imperative regardless of any warnings not to do so. Remember that any action which might be taken by a law enforcement agency will have the safety and well being of the victim as a first consideration.
2. Record the precise details of the conversation.
3. Try to remember the exact language used by the caller.
4. Note the manner of speech, speaking characteristics, accents, etc.
5. Thoroughly debrief whoever took the call to determine the type of caller and any distinctive elements of the call such as background noise which may aid in the apprehension of the caller.

ASSESSING ORGANIZATIONAL TARGETS

It is important that all key executives adopt the counter-terror security measures outlined in this guide. It is also important that executives and security advisors establish ongoing programs for identifying the specific threats to their organizations and its executives. Analysis of the media and of terrorist propaganda, liaison with appropriate law enforcement agencies, and a careful review of organizational and individual activities that are known to be contrary to terrorist positions must be conducted.

Terrorists select targets very carefully, concentrating on those individuals who will be of the greatest political propaganda value to them and on those situations which assure them of a strong likelihood of success in the attack. It is critical, therefore, that security advisors think like terrorists to evaluate likely targets. When adverse publicity is directed at the organization or its executives, it is especially important that security be increased.

END

7. 10. 19. 11. 11. 11.