

DEPARTMENT OF THE ARMY Mr. Skidmore/aeh/5291
HEADQUARTERS, U. S. ARMY TEST AND EVALUATION COMMAND
ABERDEEN PROVING GROUND, MARYLAND 21005

AMSTE-SE

14 JUL 1978

SUBJECT: Physical Security Officer's Handbook

SEE DISTRIBUTION

1. The purpose of the attached handbook is to provide USATECOM Physical Security Officers with a ready source of guidance-type reference material that will:
 - a. Aid in application of technical standards, specifications and procedures.
 - b. Facilitate more cost effective selection and application of physical security equipment.
2. This handbook represents an assemblage of data on physical security equipment from various sources. It is hoped that improvement of this guide will become a group effort within USATECOM and that it will be enlarged or continually improved through recommended changes by all elements of this command.
3. Appendix B was included, in spite of some redundancy, to provide current state-of-the-art information on several existing or potentially available systems, and more importantly, is intended to serve as a format guide for the collection and formal or informal submission of data on other systems by USATECOM Physical Security Officers. In this way the handbook can be enlarged to an even more useful document which has no known precedent within Department of the Army.
4. Portions of this guide contain For Official Use Only or Proprietary Information. As this document is expanded to include more sensitive systems and their vulnerabilities, portions of the document will undoubtedly

35613

14 JUL 1976

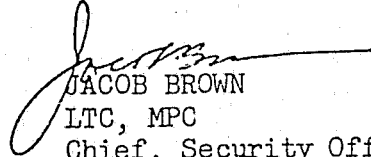
AMSTE-SE

SUBJECT: Physical Security Officer's Handbook

become classified. It is therefore incumbent upon each holder to insure appropriate designation and protection of information submitted for inclusion or which is already contained in the handbook.

FOR THE COMMANDER:

1 Incl
as


JACOB BROWN
LTC, MPC
Chief, Security Office

DISTRIBUTION:

B1, ATTN: Physical Security Officers

NCJRS

AUG 5 1976

ACQUISITIONS

PHYSICAL SECURITY OFFICERS HANDBOOK

CONTENTS

	Paragraph	Page
CHAPTER I. PHYSICAL SECURITY		
General Discussion	1	1
Barriers	2	2
Protective System Neutralization	3	4
CHAPTER II. INTRUSION DETECTION ALARM SYSTEMS		
General	1	5
Detection Devices	2	6
The Responding Device	3	21
The Transmission System	4	22
The Supervisory Program	5	23
Outdoor Perimeter Protection	6	24
CHAPTER III. SELECTING AND INSTALLING INTRUSION DETECTION SYSTEMS		
Basic Considerations	1	25
Cost Estimates and Procurement Factors	2	27
CHAPTER IV. OPERATING AND MAINTAINING INTRUSION DETECTION ALARM SYSTEMS		
Control Points	1	29
Response Factors and Backup Protection	2	30
Day-Night Control	3	31
False Alarms	4	31
Maintenance of Systems	5	31
Operational Records	6	32
ILLUSTRATIONS: TABLE 1, DEVICES, APPLICATIONS AND EVALUATIONS		
APPENDICES:		
APPENDIX A. LIST OF MANUFACTURERS		
APPENDIX B. INTRUSION DETECTION ALARM SYSTEM IDENTIFICATION AND EVALUATION		

APPENDIX C. INTERIM FEDERAL SPECIFICATION -
ALARM SYSTEMS, PROTECTIVE, IN-
TERIOR. (SECURITY)

APPENDIX D. DRAFT GUIDELINE SPECIFICATIONS
(USATECOM INTERNAL USE ONLY)

~~CHAPTER I~~
~~PHYSICAL SECURITY~~

1. General discussion.

a. Physical security is defined as that part of security concerned with the physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material and documents, and to guard them against espionage, sabotage, damage and theft. In actual practice physical security becomes a system of concentric protective barriers between a potential intruder, unauthorized person, or security hazard and the matter to be protected. These barriers may be natural, structural, animal, human or energy. They must be utilized, however, in a manner that will: physically delay or psychologically deter the intruder from approaching or entering the area being safeguarded; deny him the opportunity to exercise any of his senses or artificial devices to acquire information being safeguarded; advertise his entry or attempted entry into a protected area; or preclude accomplishment of any combination of the above objectives. It should be emphasized that physical barriers only impede and deter, but cannot be expected to do anything more than discourage the undetermined and delay the determined.

b. A problem with the discussion of physical security is one of defining the security interest and then developing an analysis of the threat to this security interest. Within USATECOM and DOD, for that matter, overall hazards considered as a basis for physical security measures fall within the following four classes:

- (1) Espionage.
- (2) Sabotage.
- (3) Various possible problems created by individuals intent on disruption or harassment activities.
- (4) Theft or pilferage.

In order to accomplish his mission successfully, an espionage or sabotage agent or thief, must have access, either direct or indirect, to the information or material he desires. The nature of the access required will depend on a number of variable factors, and may be accomplished in a number of ways.

c. In most cases of espionage the acquisition of information is the ultimate end. The means by which it is acquired are merely operational details. Normally, information recorded on magnetic tape or photographic film is as usable to the power employing the agent as the original document. Therefore, in considering access, one must consider not only

physical access to the area in which classified matter is located, but also the possibility of gaining access to such information through clandestine introduction and employment of audio or visual surveillance monitoring systems. These considerations are essential elements of physical security,

d. Within the USATECOM environment we must also be concerned with another form of espionage--Industrial Espionage. This may be defined as the illegal or unethical collection of valuable company information and data which may be used by unscrupulous competitors to the detriment of the company. Within this command it is occasionally possible for one company to illegally acquire proprietary information belonging to another company. Such thefts could easily involve defense information.

e. The real goal of both of the above forms of espionage is not only to gain information, but to obtain it surreptitiously. Some of the traditional methods used to gain this information are:

(1) Bribery of janitors and charwomen to save contents of office wastebaskets or to do other seemingly innocent tasks.

(2) Interception of mail.

(3) Clandestine listening devices (bugs, tapes, recorders etc).

(4) Fraudulent entry (misrepresentation and impersonation).

(5) Surreptitious entry (over a fence, through a door etc frequently after temporarily by passing intrusion detection alarm systems or other physical security devices).

(6) Undercover operations (getting a job as technician, engineer, maintenance personnel, etc., as a means of gaining access and freedom of movement in the target area.

f. Each of the above methods can be negated by one of two ways.

(1) By protecting the security interest with enough obstacles to penetration which will make trespass unprofitable in terms of gain or risk.

(2) By controlling people to restrict their freedom of movement and access to the security interest.

2. Barriers.

a. There is no impenetrable barrier. If a government or organization is willing to devote enough time, money, personnel, material and imagin-

ation to by-passing a barrier it can do so. Therefore, rather than attempting to achieve exclusion through use of a single barrier, security must be built upon a system of "defense in depth," or accumulated delay times.

b. Although no single barrier will deny access to unauthorized persons, it will provide a measurable minimum delay time. This delay time usually will be indirectly proportional to the skill and ability of the deliberate intruder. The measurability of this delay time may be hindered, in some instances, by unauthorized persons being able to breach the barrier inadvertently. However, certain minimum delay times have been or can be established through test and evaluation.

c. To achieve optimum results from a physical security system, it is necessary to add one barrier to another until delay times, when added together will deny or greatly impede unauthorized access. In many applications, the total delay time may be greater than an arithmetical sum of individual delays. This can be accomplished by interrelating the barriers employed. For example, an unguarded fence will provide a relatively short delay time. If that fence is patrolled by reliable guards who bring every portion of the fence under observation within the delay time the fence provides, the total delay time is greatly increased. The same guards patrolling at the same rate and frequency in areas where they can't see the fence would provide very little delay time.

d. In some cases it is necessary to differentiate between the necessity for denial of access or the necessity of being made aware that access has been gained. A further distinction is sometimes necessary as to whether it is desirable to alert the intruder to the fact that his entry has caused an alarm. When access to the security interest is gained by entry into an exclusion area it is essential that access be prohibited. It is also essential that any individuals gaining unauthorized access be apprehended and the extent of compromise established. This would preclude any system which would alert the intruder. In less sensitive areas it is frequently desirable to protect against entry by persons intent on larceny, sabotage or malicious mischief. In such situations, an audible alarm used in conjunction with other systems will often discourage such attempts. The reliance which can be placed on such "local alarm systems" is dependent upon timely response to alarms by on-site personnel or by persons normally close enough to hear and report them. Sabotage is by no means limited to the activities of foreign agents. Damage can be done by a disgruntled employee, members of dissident or anti-war groups and sympathizers, and mentally disturbed individuals, unable to differentiate between right and wrong or to consider the consequences of their actions. It is significant, however, that personnel in all of these categories are very often readily exploitable by the agents of foreign powers.

3. Protective system neutralization.

a. The possibility of intrusion detection alarm system neutralization is a basic threat and must be considered in all applications of such systems. Although these systems are designed to improve security against intrusion, the potential intruder must be regarded as an intelligent, technically competent individual who has determined or will search for means to negate the effectiveness of the system. While security personnel must insure security on all sides of the defined security interest, the potential intruder need find only one weak point or "chink in the armor." This is much easier than the security engineers job of creating a new system or eliminating inadequacies in an existing system. In devising a system for neutralization of a barrier, the intruder has not only his own initiative and inventiveness to rely upon but also the errors of security personnel who designed the system and of those who maintain it. The most vulnerable element of an intrusion detection system to neutralization is the transmission line between the alarmed area and the annunciator panel or alarm device. It is axiomatic that the sensitivity or value of material being protected will determine the sophistication and type of system employed and the degree of transmission line supervision (physical or electronic) required.

CHAPTER II
INTRUSION DETECTION ALARM SYSTEMS.

1. General.

a. Intrusion detection or protective alarm systems provide an electrical and/or mechanical means of detecting and announcing proximity or intrusion which endangers or may endanger the security interest being protected. These systems, when properly utilized in a security system, constitute a valuable adjunct to the basic security element, the guard force. Alarms possess no inherent capability to provide security other than the deterrent influence they might create. However, when integrated into a preplanned or existing security system they serve one or more of the following purposes:

(1) Permits more economical and efficient use of manpower by substitution of mobile responding guard units for larger numbers of fixed guards and/or patrols.

(2) Takes the place of other necessary elements of physical security which cannot be used because of building layout, safety regulations, operating requirements, appearance, cost, or other reasons.

(3) Provides additional controls at vital areas as insurance against human or mechanical failure.

b. The outstanding advantage of an intrusion detection alarm is measurable reliability. Although there is a wide range of complexity between the various alarm systems, test and evaluation information is usually available or can be obtained to determine what degree of security can be expected from the device. This determined degree, high or low, can be expected for most situations that the alarm would be expected to encounter. While a particular alarm system does not have the thinking and reasoning capability possessed by a human guard and, consequently, cannot be used in a comparable variety of situations or, in some cases, not at all; neither does it have the variation of response to given stimuli. The protective alarm, good or bad, is reasonably consistent.

c. The application of a particular system (or combination of systems) in a specific situation is a highly specialized matter requiring careful consideration of all factors that will affect the system operation and usefulness. These factors are discussed in greater detail in a subsequent portion of this handbook.

d. A protective alarm system is usually made up of four parts:

(1) The detection or triggering device. This is the component which detects the situation for which it was designed. It initiates the signal that will ultimately provide the alarm.

(2) The responding or alarm device. This component is a device that receives the alarm signal and converts it into a usable response designed to correct or allow correction of the undesirable situation which has been detected.

(3) The transmission system. This component transmits or transfers the initial signal to the location at which the alarm is sounded.

(4) A supervisory provision. This component, although not required for routine operation of the system, is necessary to provide an immediate means of determining that the system has become inoperative and/or to provide a self-contained power source to make available the necessary operating voltages in the event of a power failure. This provision is often integrated into the responding device to allow an alarm in the event of failure. In some systems, this provision will be coupled to the transmission system to alarm if there is tampering with the wire lines evidenced by a certain increase or decrease in the amount of current flow, in addition to announcing a complete cessation of functioning.

2. Detection devices.

a. Detection devices are usually designed to detect a single phenomenon. The choice of what type of detection device is to be employed is based upon what will be most readily detectable in the given situation. It may be desirable, in some cases, to employ more than one type of detection device to protect against all possible methods of entry. Usually, similar equipment is manufactured by several companies. Such equipment will operate on the same basic principles, but may very well differ in refinements. These differences may, under certain circumstances, alter the degree of security provided.

b. Electro-mechanical or current continuity devices are designed to effectively place a current-carrying conductor in a position which stands between the intruder and the enclosed area to be protected. In each case, the conductor carries current that retains a holding relay in the open position. A cessation of the current flow in the device releases the relay and allows its contacts to close, which closes the alarm circuit and provides the alarm. Current continuity devices may be of the following types:

(1) Metal tape or foil. This type of device is a thin strip of metal foil which is applied to the glass surface of windows or glass doors in a continuous pattern beginning and ending at contact points providing voltages of opposite polarities to cause a continuous flow of

current through the foil. The object is to arrange the pattern of the foil in such a way that breaking the window will break the foil and will, as a result, cause a cessation of current flow.

(2) Screen. This device is simply a lacing of a conductor back and forth across an area of structural weakness in such a way that cutting or breaking through the barrier would also break the conductor and cause a cessation of current flow. The screen is often applied to door panels, since they are usually weaker than the walls of the room or the remainder of the door. It may also be constructed within walls, ceilings, etc. to detect entrance made through these building surfaces.

(3) Contact switches. Contact switches are electrical contacts emplaced in such a position on doors, windows, or other openings capable of being closed, that when the opening is closed the switch is closed and there is a continuity of current flow in the circuit to the holding relay. However, when the door or window is opened, the contacts separate and the resultant cessation of current flow activates the alarm. These devices are sometimes manufactured with two separate circuits operated by two switches. The first circuit is a current continuity circuit as described above. The second circuit is a portion of the alarm circuit which provides a normally open switch connected parallel to the open holding relay and physically located at the door or window in such a way that opening the door or window will cause the switch to close. Thus, opening the door or window will open the current continuity circuit and close the alarm circuit in two ways: first, by means of the holding relay and secondly, by physical closure of the switch parallel to the relay contacts. Contact switches are of two general types:

(a) Simple contact. The simple contact switch is designed so that the movement of the door or window either physically releases a bind tension on one of the contacts and allows a constant spring tension to move this contact from its electrically closed position, or the movement of the door or window physically removes the contact affixed to it from its counterpart on the window or door frame.

(b) Magnetic contact. This device is composed of two self-contained units--a switch unit and a magnetic unit. One unit is emplaced on the door or window frame and the other on the door or window in very close proximity to the first. The switch unit contains the contact switch which, when unaffected by the magnetic unit, is held in an open position under spring tension. When the switch unit is moved to a position adjacent to the magnetic unit, the pull of the magnet overcomes the spring tension and closes the switch. This is the normal guarding position. Opening the door or window removes the switch from the magnetic influence of the magnetic unit and allows the switch to open, which provides a break in the circuit of which the switch is a part, with a consequent cessation of current flow to operate the alarm.

(4) Vibration detector. The vibration detector is a self-contained switch in a small housing unit. One contact of the switch is a small pendulum-like weight which is held under slight spring tension in contact with the other switch contact and maintains a closed electrical circuit. An attack on the surface to which the device is attached causes vibrations which swing the pendulum away from its normal position, opening the circuit and causing an alarm. This device is used as a measure of protection against attack through walls, ceilings, and extensive glass surfaces.

Since current continuity devices serve merely to close a circuit, they are vulnerable to being passed by attaching a jumper wire around the device, parallel to it. Although in theory the installation procedure is such that access to the electrical components is denied an intruder, this is sometimes difficult to accomplish. In addition, the establishing of a parallel jumper can be accomplished some time prior to the expected intrusion by a person who can gain access to the windows, doors, or electrical circuits during the normal operating hours of the office or building, for use during periods of greater privacy.

c. Photoelectric detection devices are designed to transmit a beam of light from a light source to a light-sensitive receiver, which will, in turn, react to a cessation or substantial decrease of received light. This reaction results in the initiation of the alarm signal. The components are arranged in such a way that the beam of light crosses the approach to the area to be protected.

(1) The basic requirement of this system is that the wave lengths of the transmitted light be compatible with the receivable frequencies of the photoelectric cell in the receiving unit. This presents no particular problem, however, since most light sources cover essentially all of the visible spectrum and are also richer in rays of lower frequency than visible light, i.e. infrared. Most photoelectric cells react to both infrared and visible light. The receiver operates by receiving the light and, by means of the photoelectric cell, converts the light energy into electrical energy which is used to establish an electrical situation that may be considered as normal and from which variations may be measured. Large variations in the amount of light received by the photoelectric cell produce variations in the output of the unit and are transmitted as the initial alarm signal.

(2) This basic arrangement of light source and receiver is sufficient to provide a signal when the light beam is broken and is often used in this simple and unmodified form for door opening and similar purposes, but to be at all effective as a protective alarm, certain modifications are necessary.

(3) If the light beam is visible, it may be avoided by the intruder. For this reason, infrared filters are usually placed over the

light source so only light invisible to the human eye is transmitted. Since photoelectric cells are sensitive to infrared, no modification to the receiver is necessary. The attenuation of the visible light, however, results in less light energy reaching the receiver. Therefore, either the light source must be increased, the received signal must be more greatly amplified, or the system must operate at a reduced range.

(4) Since the receiver operates normally on received light energy, any light source, visible or infrared, with sufficient strength could satisfy the requirements. Thus, the intruder, after locating the receiver, could tape a flashlight across the receiving aperture and break the beam from the system light source at will, the flashlight now fulfilling the light requirements of the photoelectric cell. To counteract such possible action, it is necessary to alter the transmitted light and to make the receiving unit selective so it will accept the light from the system light source but will not operate normally if the received light differs from the transmitted light. This requirement is fulfilled currently by modulating the light source to a frequency for which the receiver has been tuned.

(5) The simplest means of modulating the transmitted light is to beam it through a propeller-like baffle which is spun by an electric motor. The receiver must be tuned to a frequency span which will match the revolutions per minute of the motor and will also include foreseeable variations in motor speed caused by temperature change, lubrication status, and wear.

(6) A more recent method of accomplishing the modulation is to modulate both the transmitter and receiver with a signal from an oscillator connected to both. This provides a more accurately modulated signal and allows the receiver to be selective not only from the standpoint of frequency, but of phase.

(7) Another system which is currently employed to counteract the utilization of a flashlight to bypass a photoelectric detection device is the insertion of an opaque shield containing a small aperture immediately in front of the photocell. The aperture is located at the focal point of the lens of the receiving element when the light source is located, for all intents and purposes, at infinity. Unless the light source is located on the center axis of the lens, the focused light will not strike the aperture. However, this arrangement does not satisfy a situation in which the flashlight is held in front of and within two or three inches of the lens. Since the lens is focused at infinity, bringing the flashlight into such proximity to the lens allows a wide spread of unfocused light to fall on the baffle (since the focal point has now moved a considerable distance to the rear) and allows sufficient light to pass through the aperture to satisfy the re-

quirements of the photocell. If a photoelectric detection device using non-modulated light must be employed, it is necessary to emplace the receiving unit so that it is not possible to reach it without crossing the beam. This is best accomplished with mirrors.

(8) Photoelectric detection devices may be used indoors and outdoors. Exterior units are designed to provide the units with protection against the elements. Some are equipped with self-contained heaters to maintain a reasonably constant operating temperature. To allow other than a single straight beam of light, mirrors are provided to reflect the beam through the desired angular displacement. By using the mirrors, the beam may also be zigzagged back and forth across a room to make it more difficult to avoid. The effective range of the system is decreased by use of the mirrors, however, due to the light loss during reflection.

(9) As a protective alarm detection device, the photoelectric system can be considered as little more than supplemental. In spite of its using invisible light the infrared beam can be detected by a metascope and will cause an indication on a sensitive photographic exposure meter. To operate, it must have its telltale apertures and, in many cases, mirrors to provide a path for the light, even when the equipment is concealed. The effective width of the beam is usually less than six inches and, once located, can be avoided. Although it would involve some equipment and trouble, the modulated light can be duplicated by using a sampling of the transmitted beam to trigger an electronically modulated light source carried by the intruder, to satisfy the requirements of the tuned receiver. Except for this latter possibility, the photoelectric system is highly effective against vehicular movement through it, since it is impractical to attempt to move the vehicle over or under the beam. Although the system may be effective for vehicles the effectiveness may be limited to a given situation by the possibility of stray animals or flying matter passing through the beam, thereby causing false alarms.

d. Proximity detection devices: operate by surrounding an object with an electrical field in such balance that absorption of some of the produced energy by the entry of an electrically conductive body into the field creates an imbalance in the system that results in the initiation of an alarm signal. Although the results of the systems are essentially the same, there are two operationally different types of proximity alarms:

(1) The electromagnetic detection device is basically a low power, low frequency radio transmitter with two receivers tuned to net with the transmitter. The detection field is established by three parallel wires, the center wire being an antenna to the transmitter and the two outer wires antennae to the two receivers. In operation, the transmitter transmits a radio signal causing electromagnetic waves to radiate concentrically from its antenna. These waves are inductively received by the

outer wires and create voltages which are received and detected by the receivers. In tuning the system the output voltages from the receivers are made equal and opposite and fed into a comparison circuit where they cancel, causing an absence of output from the comparison circuit. If a conducting body moves into the radiating field of the transmitter so that some of the energy destined for one of the receiving antennae is absorbed, the output from that receiver is less than the output from the other receiver. This reflects itself at the comparison circuit as a difference in voltage and an output from the comparison circuit results. This output is the initial alarm signal. Since the center wire is a transmitting antenna, it must be properly tuned to effectively radiate its generated energy. Ideally, this is accomplished by achieving a precise length of wire which will cause resonance for the frequency at which the transmitter is being operated. Since this is not always practical, a loading coil is used to create a theoretical length to provide the resonance. Loading the antenna in this manner greatly attenuates the transmitted signal at shorter wire lengths to a point at which the device is no longer effective. The minimum length of antenna will depend, of course, upon the transmitting frequency and the tuning arrangement, but it can be safely said that an antenna shorter than 50 feet would render the device ineffective.

(2) The capacitive (electrostatic) detection device operates superficially in the same manner as the electromagnetic including in some applications, the use of the three parallel wires. The capacitive alarm is generally more versatile than the electromagnetic since it does not require the lengths for tuning that the electromagnetic device does. The capacitive detection device is, in effect, a large electric condenser which radiates as does its smaller counterpart, electrostatic lines of force created by a build-up of electrons on one plate which is separated from its second plate by air as a dielectric. There are several possible applications, but each involves a conducting body moving into the electrostatic field after a balance has been achieved and absorbing some of the energy to disrupt this balance. The situation resulting here is similar to that brought about when one moves close to an old radio and hears a squeal. The energy absorbed by the body causes an internal circuit to break into oscillation creating an initial alarm signal. Some systems of this type provide a second plate in the form of a wire or grid separated from the first, which can also be a wire or can be a metal cabinet. Other systems dispense with the second plate and let ground fulfill this function.

(3) Both the electromagnetic and the capacitive systems lend themselves well as fence alarms. Since the alarm signal is created by mere proximity to the wires, it is essentially impossible to tamper with the detection device. Attempting to tamper with the wires by standing outside the field and cutting the wires with a long-handled non-conducting instrument is equally unproductive, since the changing of the

wire length would create the alarm signal. As fence alarms, the wires are either strung on insulated brackets on an existing perimeter fence or established on their own poles as a purely alarm-type fence. When installing this device, care must be exercised to devise a means to preclude the alarm's being set off by curious or mischievous persons just to see guards come out. It is desirable to have a definite barrier between the fence and areas of uncontrolled traffic.

(4) The capacitive detection device is also effective for interior use. The wires can be strung across banks of windows or around door frames. It is frequently used as a cabinet alarm for one or more metal cabinets or safes which are wired as the charged plate so the alarm signal will be initiated when a person approaches them.

e. Acoustic detection devices are those devices that are actuated by the sound or vibrations made by the intruder during his approach or as a result of his attempt to gain entry. The principles of operation of this type of device are comparatively simple. Regardless of application, sound waves or vibrations are picked up by a microphone which converts them to electrical energy. This electrical energy is amplified and transmitted to a receiving apparatus which reconverts the electrical signal to sound waves similar to the original. The receiver also may use the electrical energy to actuate an alarm device.

(1) When applied so that a reproduction of the original sound is required to be transmitted to a remote location, the detection device will consist of one or more reasonably sensitive microphones, capable of accepting sound waves in the audio range, and an audio amplifier to increase the electrical signal to a level which would allow transmission to the remote location. This detection component then feeds into a transmission link (radio or wire). The signal ultimately arrives at the remote receiver where it is transformed into audible sound waves. Those sounds, capable of being heard by a person in the vicinity of the sound source should also be detected by the system. Lower level vibrations in the walls, ceilings, or floors, resulting from an attack on these surfaces, may not be transmitted if there is insufficient sensitivity in the system.

(2) When applied in such a way that a reproduction of the original sound or, in this case, vibration of a building surface is used to actuate an alarm device, contact microphones should be strategically located on those portions of the building surfaces capable of measurable vibration. Since these contact microphones would not cause an alarm from reception of low or normal level sounds within the room, ordinary audio microphones

may also be employed. This application is designed to detect the attempt at entry by a means which would create a registerable sound or vibration, such as cutting, ripping, jimmying, or other forceful entry.

(3) The above two methods are often combined to allow an alarm to be actuated by sound or surface vibration in order to attract the attention of the guard, and to allow him to monitor an audio reproduction of original sound to provide a remote check of the cause of the alarm.

(4) In exterior applications the acoustical alarm may be used underground to detect the surface approach of an intruder or to detect digging or tunneling operations in the vicinity. In this application, the use of more than one microphone or transducer is required to allow a signal comparison and neutralization in the event sound is received from aircraft, traffic, or other distant source of loud sound. An alarm caused by such sound sources would be undesirable, and yet the desired sensitivity would allow such false alarms if a means were not employed to prohibit them. By comparing the signals received from more than one microphone it is possible to cancel a signal caused by a sound which reaches two or more microphones with approximately equal intensity, thereby limiting the sounds causing the alarm to those occurring close to the microphone.

(5) Acoustic detection devices, for the most part, can be applied to quiet areas only. With the exception of those employing cancellation circuits, all are susceptible to causing false alarms when innocent sounds or vibrations occur. The sensitivity of these devices must, for this reason, be set at a level to allow normal sounds without setting off the alarm. Consequently, if the intruder were aware of the existence of the acoustic device, he could possibly govern his actions to maintain a required level of quiet.

f. Movement detection devices are designed to create an alarm when there is movement of any sort within the established limits of the device. There are several types of movement detection devices--sonic, ultrasonic, radar and optical.

(1) Operation of the ultrasonic and radar devices is based upon a principle called the Doppler effect. The principle of the Doppler effect is that when a source of transmitted waves, either electrical waves or sound waves, and the receiver of the waves are moving toward or away from each other, the received signal will be of higher or lower frequency, respectively, than the transmitted signal.

(a) In the case of the transmitter and receiver moving toward each other, the distance moved during the period of time between wave emissions is subtracted from the actual length of the transmitted wave, giving the transmitted signal, in effect, a shorter wave length and consequently, a higher frequency or, in the case of sound waves, a higher pitch.

(b) Just the opposite is true when the transmitter and receiver are moving away from each other. In this case, each successive wave has to travel farther than the preceding one before it is received. This results in a longer wave length than the designed wave length and a resultant lower frequency.

(c) The same principle is applied in a situation in which both the receiver and transmitter remain stationary, but in which there is a moving object, capable of reflecting the waves from the transmitter to the receiver. In this case, the receiver sees the reflecting object as the transmitter, since it is from the reflecting object the signal is received. Thus, in theory, if the reflecting object is moving toward the receiver, the received signal is of higher frequency than the transmitted signal, and if the reflecting object is moving away from the receiver, the received signal is of lower frequency than the transmitted signal. In actuality, there will be two frequency changes in this case. The reflected signal will differ from the transmitted signal because of the movement of the reflecting body in relation to the transmitter, and the received signal will differ from the reflected signal because of the movement of the reflecting body in relation to the receiver. The direction of movement in relation to both the transmitter and receiver will determine whether these differences are added together or subtracted from one another. The only situation in which one would cancel the other would be when the reflecting body is moving along a straight line between the transmitter and the receiver.

(2) The ultrasonic movement detection device is so named because it employs sound waves above the audio range; i.e. of a frequency higher than the human ear is capable of receiving. In operation, the ultrasonic device transmits a sound tone which permeates the room in which it is contained with sound waves. These sound waves are received directly and reflectively by a receiver. Samples of both the transmitted signal and received signal are fed to a comparison circuit. As long as there is no movement in the room, the received signal, including both the waves received directly from walls, ceilings, floor, and objects in the room, is of the same frequency as the transmitted signal and the two compared signals at the comparison circuit cancel out. When there is movement in the room, the signals received directly from the transmitter and those reflected from stationary surfaces and objects remain unchanged; however, those signals reflected from the moving object will differ and the resultant signal sent from the receiver to the comparison circuit will differ from the signal sent from the transmitter to the comparison circuit. This results in an incomplete cancellation and the initiation of the alarm signal.

(a) Since a single ultrasonic transmitter has its range limit, it is necessary, in larger rooms or areas, to use more than one transmitter and receiver. The construction and contents of the room will also have

an effect upon the volume a single unit is capable of filling with sound waves. Empty rooms, without structural obstructions, attenuate the sound waves far less than rooms with heavy drapes, soft furniture, rugs, etc., since these objects absorb or muffle some of the sound. Determining the unit requirements for such installations requires a survey by personnel qualified in this field, usually contractor personnel.

(b) This device is unaffected by exterior noise in the audio range. It reacts only to movement within its area. It can be adjusted to such a degree of sensitivity that the movement of air caused by fire, or by air conditioning, will activate its alarm. It is a very effective detection device for the security of a closed area since it will not only alarm when a door is opened or when a wall is broken through, but will also cover the eventuality of the stay-behind intruder, the intruder who entered the room when it was open for operation and hid himself there. It will not, however, alarm if cabinets or containers placed flush against a wall are attacked through the wall, since no movement is executed in the path of the sound waves. The protection provided by this device is contained by the walls of the area in which it is operating. Consequently, it will not cause false alarms because of movement beyond the walls.

(3) The radar movement detection device operates on essentially the same principle as the ultrasonic. The difference is the type of wave employed. While the ultrasonic uses a sound wave, the radar device uses an electronic wave of extremely high frequency, usually in the frequency spectrum of around 350 megacycles per second. The radar detection device transmits its signal, which is reflected back to its antenna and is received by a receiving unit. A comparison circuit compares the transmitted and reflected signals, from the standpoint of phase shift of the electronic waveform. If there is no movement in the area the waveform remains constant in its phase relationship; however, when the beam is reflected from a moving object, the phase of the reflected wave will shift; i.e. the positive and negative peaks will occur at a slightly different point in time from the point at which they would have occurred had the object not been moving at the time the wave was reflected. As with the ultrasonic, this difference in the received reflected wave causes a difference in voltage, which becomes the initial alarm signal. The employment of a radar wave, as opposed to a sound wave, creates several operational differences between ultrasonic detection and radar detection.

(a) While the sound waves are contained within an inclosure of any solid material, the radar waves will penetrate many substances. Plaster walls, for example, will be penetrated to a high degree. A person or object moving on the outside of the plaster wall would reflect the signal through the wall once again, and would cause the device to alarm. If this characteristic is undesirable in a given situation, it is possible to decrease its effects by decreasing the power of the transmitter or by covering the walls with a metal foil through which the signal will not penetrate.

(b) The radar beam is completely line of sight because of the high frequencies employed. If movement occurred behind an object made of a material which the beam would not penetrate, e.g. a metal desk or cabinet, the movement could not be expected to be detected.

(c) Although the radar beams can be expected to be reflected to some measurable degree from any conventional solid material, radar absorbing material has been developed which can be moved within the operating field of a device of this type without registering by reflection and, consequently, without causing an alarm. A shield of this material, however, is large and bulky and, if observed, is likely to excite curiosity. In most situations the intruder would probably find such a shield awkward to transport to the area in a surreptitious manner.

(d) Since sound waves attenuate rapidly in air, a radar detection unit producing an output comparable to that of an ultrasonic unit could be expected to provide greater range for coverage of a larger area.

(4) The sonic motion detection device is so named because it uses audible sound waves, continuously transmitted within a protected area, to detect the movement of an intruder into or through the field of sound waves.

(a) The sonic detection system emits a low frequency sound which is compared with an internally generated signal. Differences detected in the phase relationship of the reflected energy are converted to voltage changes. These voltages, when sufficient, cause an alarm condition to be registered at the monitoring station.

(b) Sonic systems are best suited for areas where walls, floors and ceilings are easily penetrable or windows and doors are loose fitting. This type system can normally be expected to provide a more economical area protection system than is possible with a combination of less sophisticated devices. The area being secured should be free of any exposed moving masses such as fan blades, drapes or other objects being blown about, air currents at variable temperatures, or high-velocity air streams.

(5) Optical enclosed-space or volumetric intrusion detectors are of several types. The most frequently encountered types are:

(a) A system incorporating a balanced pair of photocells and associated sensing circuits which can detect differential changes in light intensity caused by a moving object or intruder in a controlled light environment. Uncontrolled light such as daylight will affect the operation of such systems.

(b) Another system in this category consists of a number of photo-cells mounted in a camera and a light source modulated at 60 hertz. The modulation is obtained by connecting a rectifier in series with a modulated light source. The use of a modulated light source and a timed amplifier in this system reduce the system sensitivity to outside light.

(6) Although a closed circuit television system is not, strictly speaking, an alarm device, in that it is normally not used to create an alarm signal, it is a detection and is frequently used in a physical security system to extend the function of guard personnel.

(a) A basic closed circuit television system is composed of a camera unit, a control unit, and a monitor unit. The camera converts a visual image received through its lens system to an electric current modulated in proportion to the light received. This is accomplished as the camera effectively scans parallel horizontal lines of the scene it faces in such a way that the light at the point being scanned at any one instant produces an amplitude of electrical current comparable to it. This modulated current is ultimately transferred through cables to the monitor. The monitor is a television receiver tuned to the carrier frequency of the camera. A synchronization signal is employed in the camera and the monitor to cause the sweep of the beam lighting the face of the monitor's picture tube to agree with the sweep of the camera's image converter tube. This synchronization or agreement must be such that the sweep beams begin at the same point, cross the tubes at the same rate, fly back at the same rate to the same relative position on the next lower level, and proceed in this manner until the field of the camera and the picture tube have been covered, at which time the process is repeated. Since the light from the scene is modulating the beam of electrons sweeping the face of the picture tube, this beam is able to paint its picture in lights and darks as it sweeps back and forth across the tube. The control unit is used to make adjustments to the variables of the camera's operation. Various lenses and accessory equipment may be employed to allow the system to fulfill the installation's requirements.

1. The camera unit can be equipped with several types of lenses in much the same way as a motion picture camera. There are available, in addition to the normal lenses, wide-angle lenses to increase the field of view and telephoto lenses to effectively bring the viewer closer to the scene. Lenses are available in several focal lengths to allow for the desired wide-angle or telephoto effect. Some cameras are equipped with lens turrets to allow wide-angle, normal, and telephoto lenses to be interchanged rapidly. Zoom lenses are also available to allow changing the received picture effect from wide-angle through normal to telephoto with the single lens. Any effective focal length between the designed extremes may be chosen to provide a picture of the desired field or magnification.

2. Remote control equipment which may be desirable includes a remotely controlled pan and tilt pedestal, which allows positioning the camera in the desired horizontal and vertical direction from a remote location. The lens turrets and the zoom lenses may be remotely controlled so routine observation covers a wide field of view but the telephoto effect may be used to provide closer observation of a suspect area or person. A scanning mechanism causes the camera to turn at the rate of about 2 RPM to provide all-around observation. Accessories to protect the camera equipment from the weather are necessary for outdoor installation.

(b) The closed circuit television has four guarding advantages capable of exploitation in a security system.

1. The use of cameras in several areas with corresponding monitors in one central location allows one guard to make frequent checks of these areas.

2. The cameras can be located in areas that would be hazardous to guard personnel.

3. Under extremes of temperature and climate, the use of the television system will allow the guard to be in a more comfortable location and, ideally, to be able to better apply himself to his duties.

4. By using remotely controlled lens turrets or zoom lenses, the guard is able to almost instantaneously move up visually to examine a suspicious circumstance. This, of course, can be accomplished as well by the guard in the area, if he has been equipped with comparable optical equipment.

(c) There are also several possible disadvantages to the use of a television system to replace the guard in the area.

1. The television screen will not provide as faithful a reproduction of the scene as will direct vision. For this reason small details may not be discernible.

2. Dividing a guard's attention between several monitor screens may not provide the continuity of coverage desired.

3. The resultant eyestrain and boredom of watching an area through the medium of television may cause a lack of attention.

4. The area to be viewed may contain sufficient obstructions that even several cameras could not give the coverage provided by a roving guard or guard patrol.

5. The camera is incapable of taking corrective action in the event of an undesirable situation. The time required to move a guard or guards to the area covered by the camera may be excessive.

g. Since fire is one of the simplest and most destructive methods the saboteur has at his disposal, fire detection devices must be considered as protective alarm detection devices. Devices of this type are usually designed to fulfill one function only. Fire has three detectable properties: light (visible and infrared), heat (convected and radiant), and smoke. Which of these is to be detected is dependent upon the situation at the installation being surveyed.

(1) Light detection devices operate on a photoelectric principle. The light generated by the fire is received by a photoelectric cell and converted to electrical energy to provide an alarm signal. Light detection fire alarm devices must be so selective that steady continuous light does not actuate the alarm, but that the flickering light of a flame will do so. The advantage of this type of device lies in its use in open areas or large areas which would dissipate heat rapidly. It is effective in any application in which the flames could transmit light to the device.

(2) Smoke detection devices, also photoelectric in nature, operate on the same principle as the photoelectric anti-intrusion device. This unit includes the photoelectric receiver containing the light sensitive cell and its own light source. When smoke passes between the light source and the receiver, the intensity of the received light is decreased by the filtering action of the smoke. This causes a change in the electrical output of the photoelectric cell and a consequent alarm signal. This type of device is most applicable to poorly ventilated areas, which would tend to produce smoldering fires.

(3) Heat detecting devices are of two general types: fixed temperature detectors and rate-of-temperature-rise detectors.

(a) A fixed temperature detector is a device which is capable of being set to provide an alarm when the temperature in the vicinity of the device has reached a previously selected level. These devices are usually of simple thermostatic design using metals of high coefficient of thermal expansion to cause electrical contacts to move together and close to complete the electrical alarm circuit. This type of detector can operate at various cut-off temperatures, usually in the range between approximately 140° and 350° F. The devices are employed in preference to the rate-of-temperature-rise detectors in situations where the routine operations themselves cause rapid temperature fluctuations, such as boiler rooms, annealing rooms, etc.

(b) Rate-of-temperature-rise detectors function by measuring rapid rises in the temperature in the vicinity of the device. Some devices of

this type are actuated by radiant heat, making them adaptable to large areas or to areas where the movement of air might make convection heat detection devices less effective.

(c) Any detection system composed of two detection devices, one exposed and one shielded from direct heat, can be used as a rate-of-temperature-rise detector by comparing the temperature differences. This can be accomplished by using thermocouples (joined wires of dissimilar metals) to convert the heat energy to electrical energy. In operation, when the room temperature rises slowly, the shielded device and the exposed device warm at about the same rate, but when there is a rapid rise in temperature, as would exist in the event of a fire, the exposed elements warm faster, creating a measurable difference in received heat, consequently, a marked difference in electrical output. This, in turn, provides the alarm signal.

(d) Another rate-of-temperature-rise device is the pneumatic fire detector. This system employs thin copper tubing which terminates in air chambers which are equipped with a movable diaphragm capable of closing an electric circuit when bulged. When a fire starts, the temperature in the immediate area increases rapidly. This causes the air inside the tubing to expand rapidly and to press against the walls of the air chambers. The metal diaphragm provides the line of least resistance, because of its flexibility and bulges, which close the electrical contacts and transmit the alarm signal. Slow temperature changes expand the air in the tubing slowly, but small breather vents allow sufficient air to pass in and out of the system to equalize inside and outside pressures.

(e) Sprinkler systems, although not alarm devices, both detect and combat fire. In this system, each sprinkler head located on overhead water pipes is plugged with a low melting point metal. When the temperature reaches a certain level, the metal plug melts and the water is released in a spray to extinguish the fire. In this respect, it could be classed as a fixed temperature detector, in spite of the fact that no alarm is transmitted. However, a waterflow alarm system can be used in conjunction with the automatic sprinkler system to sound an alarm when the water in the pipes begins to flow. Combining these two systems offers the following advantages in a situation in which a fixed temperature detector accomplishes the desired result: first, the automatic sprinkler system provides immediate sprinkler action as soon as the heat reaches the predetermined point and water continues to flow until manually shut off. Secondly, the waterflow alarm alerts guards or fire-fighting personnel to the flow of water, which causes them to proceed to the area so protected to hasten the extinguishing of the fire and stop the flow of water when it is no longer needed. This action reduces the damage caused by fire and by water. Finally, the waterflow alarm also detects ruptured pipes or other leaks in the system.

3. The Responding Device.

a. The basic function of a responding device or control panel is to receive the intrusion signal from the detection device and alert monitoring personnel that the protected area has been compromised by an intrusion. The manner in which this is accomplished varies with each manufacturer. In general, a buzzer or bell and a light are activated when an intrusion occurs. In addition, all operationally accepted control panels are equipped with both audible and visual signalling devices which, when activated, announce that a change of conditions or trouble has occurred in the system, such as the following:

(1) Tampering by a would-be intruder with the detection devices or reporting line, with the purpose of attempting to breach the system.

(2) Failure of component parts of the equipment to function properly (fail-safe).

(3) Failure of the power supply.

b. Another function of a control panel is to provide the electrical energy, from a central power source at police headquarters, necessary to operate the electrical components of the system. It must be pointed out that some manufacturers provide the electrical energy to operate the detection devices only, from a power source in the protected area and not from the control panel. For added protection to the entire system, all electrical power should, when feasible, be provided from the police headquarters where the control panel is located.

c. When discussing control panels, it must be pointed out that the number of control panels required in an intrusion detection system is necessarily dependent upon the number of areas to be protected and the capability of one control panel to identify alarm signals received from more than one protected areas. Some control panels can only identify alarm signals from one area, while others have the capability of identifying alarm signals from many areas. Since the capabilities of a control panel varies with manufacturers, the number of control panels required for the number of areas or zones to be identified must be determined from the manufacturer of the equipment under consideration. Thus, several control panels may be required for consolidation into one master control panel. The master control panel is usually located at police headquarters.

d. Although the responding device is designed primarily to attract the attention of guard personnel by visual and/or aural alarms, this device can also cause the performance of any single action which depends upon electrical energy for its initiation. As examples of the possible applications to which this device may be put in addition to alarm-type response, the responding device can:

(1) Turn on lights in an otherwise unlit area when intrusion has been detected in that area.

(2) Drop barriers between double fences to contain an intruder who has been detected between fences.

(3) Deadlock exits from an area in which intrusion has been detected to contain the intruder.

(4) Release guard dogs into an area in which intrusion has been detected to apprehend the intruder.

(5) Close fire doors and release extinguishing agents when flame, heat, or smoke is detected by the detection device.

e. Although the detection device is normally operated by means of commercial power, the responding device should have a self-contained battery power source, either as a primary or alternate source, to allow the employment of fail-safe circuits.

4. The Transmission System.

a. The transmission system is a means of transferring the initial alarm signal from the detection device to the responding device. Either wire or radio can be used. A radio transmission system, of course, requires a radio transmitter connected to the detection device and a radio receiver to feed the received signal into the responding device. A wire transmission system may require one or more preamplifiers to raise the initial alarm signal to a level which would overcome circuit losses in long transmission lines.

b. Although transmission systems may be typed in the manner in which the initial alarm signal is transmitted, i.e. wire or radio, for evaluation purposes it is more worthwhile to classify them in accordance with their length, or the location of the responding device in relation to the detection device. From this standpoint, the transmission systems are usually divided into two types, local alarms and central station alarms. This division, however, does not necessarily describe all types of transmission system installation. Therefore, for purposes of this text and for security survey and inspection reporting purposes, transmission system installation will be divided into three types: local, central station, and proprietary.

(1) A local alarm system is one in which the protective circuits and devices are connected to a responding device located at or in the immediate vicinity of the protected area or installation, and which is responded to by guards in the immediate vicinity. This type of installation usually alerts the intruder as well as guard personnel.

(2) The central station alarm system is limited, for purposes of this manual, to a system in which the transmission system connects a detection device located in the protected area to a responding device at a location remote to the installation. This system is usually serviced by guard personnel employed by a contracting agency, which services other similar alarm installations in the same city or area. Leased commercial telephone lines are normally used as the transmission medium.

(3) A proprietary alarm system is similar to the central station alarm system in that the responding device is at a remote location under the supervision of guard personnel. However, the proprietary alarm system differs from the central alarm system in that the remote location is on the installation being protected and the guard personnel are employed by the installation. The transmission medium may be either internal telephone circuits or separate circuits established specifically for the purpose of carrying the alarm signal.

5. The Supervisory Program.

a. The combination of the detecting device, the responding device, and the connecting transmission system creates a complete, functional protective alarm system. However, these components alone do not make provisions for the possibility of a power failure which would render the entire system inoperative. Neither do they provide warning that tampering with the components is being accomplished in such a way that the entire system may be neutralized. If the alarm system is to provide effective security, these two possibilities must be taken into consideration (when faith is being placed in an alarm system, an inoperative system is worse than none at all) and a means provided to overcome them.

b. Supervisory provisions designed to combat the possibility of power failure are relatively simple, since the difference between full normal power and a complete cessation of power is a marked one. A holding relay with contacts in series with the alarm may be used by having the power source connected to the coil of the relay. In the event of a power failure the coil would no longer hold the contacts open. Therefore, the contacts, under spring tension, would close and complete an alarm circuit operating on its self-contained battery power. This would, in turn, alert guard personnel to the power failure. A standby battery power system to replace the commercial power is advisable for operating the entire alarm system in such emergencies.

c. Although protective alarm systems will remain operative at less than full power, when power decreases the efficiency of most detection devices decreases, and with sufficient decrease the device either becomes completely inoperative or produces such a weak alarm signal that the responding device is not activated. If not included in the system it is

desirable to employ a holding relay adjusted to close its alarm circuit at a point selected to be above a minimum power requirement. In choosing this point, however, it must be remembered that if the allowable deviation from rated voltage is too small, there will be numerous false alarms caused by unimportant fluctuations. Choosing that cutoff point becomes somewhat critical.

6. Outdoor Perimeter Protection.

a. At present, there is no ideal intrusion detection device. However, there are a number of devices which can be effective when properly applied. Prime consideration in the application of these devices are the environment in which the devices are to be used and whether one device complements another. For example, seismic detection devices which are to be used for the detection of footsteps will, unless extremely good discrimination circuits are provided, be completely useless if positioned where they are influenced by the vibrations of passing vehicles. However application of these devices on the roadway and on a remote footpath could give meaningful information on both vehicle and personnel intrusions.

b. Devices available for the protection of outdoor perimeters include seismic devices, radars, magnetic loops, capacitive and transmission line fences, taut wire fences, infrared beams, magnetic loop detectors, television systems, break-wires and noise makers. These items and their application will be further described in a classified addition to this handbook at a later date.

CHAPTER III
SELECTING AND INSTALLING INTRUSION DETECTION SYSTEMS

1. Basic Considerations. The selection of any intrusion detection system basically involves a careful analysis and study of what is to be protected and the equipment most suited to provide the desired protection. Many of the systems available today are designed to be flexible and versatile in their application to USATECOM security problems so that they may be adapted to most situations requiring this kind of protection.

a. Degree of protection required.

(1) Before any system can be selected, it must first be established just what is to be protected. For example, if the security problem involves protecting highly classified documents stored within an approved-type container, it would obviously be extravagant to protect the entire room. If additional protection is required for the container, it normally could be adequately protected with a simple near field detection system. Another example might be one where a number of containers are used to secure highly classified documents or material within a walk-in type vault area in an administrative- or headquarters-type building. In this case, it would be unwise, economically, to install an intrusion detection system to protect the entire building.

(2) Conversely, a building containing a large amount of highly classified documents in many containers or safes and/or classified materials or material which cannot be secured in a vault or container, would require total area or building protection if the items could not be consolidated within a secure area. Similarly, this same method of protection may be applied to a warehouse containing sensitive materials or pilferable items easily removed from the installation by virtue of their size and weight. The examples cited above are intended only to emphasize the importance of first defining what is to be protected. The determination of the amount of protection to be provided will be discussed in the paragraphs immediately following:

b. Depth of protection.

(1) In those cases where visual or audible access would compromise activities being carried on within a building, it may be necessary to detect the approach of a would-be intruder at some distance from the critical information or material requiring protection. This could be accomplished through use of a perimeter type alarm system installed at any appropriate distance from the area to be protected. Another reason for installing a barrier type alarm system some distance from the area under protection is to provide security police force personnel with sufficient time to intercept the intruder between the fence or barrier and the

protected area and preclude compromise. However desirable this type of protection might appear to be, from a security point of view, it is expensive and difficult to maintain.

(2) Exterior or perimeter alarms do not provide security in depth. They must be used in conjunction with other more common deterrents such as fences, walls, etc. To achieve security in depth with any degree of reliability it is necessary to employ point, area or volumetric systems in conjunction with perimeter or linear systems. This provides a more cost-effective type of security following what is commonly referred to as "island security." Generally, a perimeter is more easily and economically protected by a linear type system such as: taut wire; capacitance fence; active modulated and CW light beam breakers; active modulated and CW infrared light beam breakers; passive infrared; active ultrasonic beam; differential seismic perimeter; magnetic; pressure sensing; differential seismic; balanced transmission line and radar systems. These systems are all rather easily defeated if their existence and component locations are known.

(3) Area coverage devices include seismic, vibration, switchmats, stress or strain systems, and capacitive systems. Seismic systems are very difficult to use indoors because of their sensitivity to vibrations caused by nearby traffic, rotating machinery etc. The normal building construction serves as an undesirable propagating medium for seismic waves. With the exception of seismic devices, area coverage devices are more effectively employed internally. Vibration detection systems can be mounted in a wall perpendicular to the vertical axis so that attempts to break into a vault or wall which require the expenditure of force in the horizontal plane will be detected. Capacitive systems are used primarily for protecting vaults, equipment or filing cabinets. A requisite to their use is that the surface be metallic. These types of devices, as with perimeter systems, can be circumvented by a sophisticated threat requiring careful consideration of how they may be used in combination or with other devices. Particular care should be exercised to insure compatibility of all devices used.

(4) Volumetric or internal coverage systems are available to detect motion, body effluents, (olfactronic) or sound within a volume of space to be protected. A maximum amount of coverage can be obtained with these systems making it very difficult for an intruder to gain access, no matter which path he selects. This makes volumetric systems attractive for use in any high security application. However, these systems are more susceptible to false alarms than systems providing less coverage. If this problem can be dealt with logically the volumetric alarms offer the most effective and efficient detection devices. Volumetric devices include: CW doppler radar, ultrasonic systems, antenna loading systems, acoustic (passive) systems, magnetic, balanced light and television systems.

c. To insure consideration of better-known equipment for potential application within this command, a list of security equipment manufacturers is attached at Appendix A. Each manufacturer is coded for purposes of identification with the description in Appendix B of twenty different types of intrusion detectors. Table 1 gives a general overview of a very limited evaluation of various devices. Each device is listed with an object it can logically protect and an evaluation of its effectiveness in detecting intruders (using five criteria), the effect of environment on the detector (using six criteria), and the approximate cost. Only general ratings of low, medium and high are used to indicate the relative ability of the sensor.

d. The next problem in installing alarm systems is where. Consideration must be given to where each detection device will be best located for both efficiency and economy. Since structural members of the area being protected (roof, walls, and floor) form a definable perimeter it is normally only necessary to protect apertures and the cubic space within the perimeter. Where use of a motion detection unit is employed (such as sonic or radio frequency), it may not be necessary to protect apertures since intrusion of a foreign body into the area will actuate an intrusion signal. On the other hand, where audio or capacitance systems are employed it will probably be desirable to protect apertures to detect entry at the earliest moment rather than waiting until the object under actual protection is approached. Regardless of which systems are employed, it is normally necessary to back up an interior alarm with a perimeter alarm. The problems involved in breaching two complementary alarm systems are much more complex than breaching a single system.

2. Cost Estimates and Procurement Factors.

a. In planning an intrusion detection system, a technical plan must be prepared so that an estimate of equipment and installation costs may be determined and program approval obtained from this headquarters and OPMG, DA. Although acquisition and installation costs of reporting lines present no particular problem, such is not the case with detection devices and control panels. By the very nature of their design and wide divergence of their capabilities in terms of range, coverage, limitations as to zones, etc., it is virtually impossible to estimate the cost of such equipment without personal contact with the manufacturers. While it is true that all manufacturers provide literature concerning their products, such information is generally inadequate in providing sufficient information upon which to determine the amount and type of equipment required and its cost.

b. Experience has shown that it is virtually impossible to provide even very general guidelines to be used in developing a cost estimate. This is brought about by the fact that when a manufacturer claims his product will protect a given number of square feet, the

TABLE 1. DEVICES, APPLICATIONS, AND EVALUATION

ITEM	DEVICE	APPLICATION	EVALUATION																
			EFFECTIVENESS					ENVIRONMENT						UTILITY		COST			
			Confidence that intrusion will be detected	Resistance to defeat	Difficulty to observe	Operating reliability	Freedom from false alarms	Immunity to air turbulence	Immunity to noise (acoustic)	Immunity to noise (vibration)	Immunity to noise (electrical monochromatic)	Immunity to noise (electrical impulse)	Immunity to temperature changes	Ease of installation	Ease of calibration		Ease of maintenance		
1.	Mechanical switches (all types)	Doors, windows	H	L	L	H	H	H	H	H	H	H	H	H	H	H	H	H	\$ 40
2.	Magnetic switches (unbalanced)	Doors, windows	H	L	L	H	H	H	H	H	H	H	H	H	H	H	H	H	50
3.	Magnetic switches (balanced)	Doors, windows	H	L	L	H	H	H	H	H	H	H	H	H	H	H	H	H	30
4.	Infrared break beams	Doors, windows, openings	H	L	M	M	H	H	H	M	H	M	H	M	H	M	H	M	300
5.	Infrared break beams	Passages	H	L	M	M	H	H	H	M	H	H	H	M	H	M	H	M	300
6.	Infrared break beams	Containers	H	L	M	M	H	H	H	M	H	H	H	M	H	M	H	M	300
7.	Active infrared single sensor	Floors, windows, openings	H	H	H	H	M	H	H	H	H	H	H	M	H	L	H	L	1,200
8.	Active infrared single sensor	Passages	H	H	H	H	H	H	H	H	H	H	H	M	H	L	H	L	1,200
9.	Active infrared single sensor	Space	H	H	H	H	H	H	H	H	H	H	H	M	H	L	H	L	1,200
10.	Active infrared single sensor	Containers	H	H	H	H	H	H	H	H	H	H	H	M	H	L	H	L	1,200
11.	Active optical dual sensor	Space	H	M	H	M	L	M	H	M	H	H	M	M	M	M	M	M	300
12.	Active optical multiple sensor	Space	H	M	H	M	M	H	H	M	H	H	H	M	M	M	M	M	400
13.	Passive IR detector dual beam	Doors, windows, openings	H	H	H	H	H	H	H	H	H	H	H	M	H	L	H	L	600
14.	Passive IR detector dual beam	Passages	H	H	H	H	H	H	H	H	H	H	H	M	H	L	H	L	600
15.	Passive IR detector dual beam	Containers	H	H	H	H	H	H	H	H	H	H	H	M	H	L	H	L	600
16.	Passive IR detector cone beam	Space	H	H	H	H	M	M	H	H	H	H	H	H	H	L	H	L	1,100
17.	Passive IR detector fan beam	Space	H	H	H	H	H	H	H	H	H	H	H	H	H	L	H	L	1,100
18.	Motion detecting TV	Space	M	M	L	M	M	H	H	M	H	H	H	L	M	L	H	L	10,000
19.	Break wire	Doors, windows, openings	H	L	L	M	H	H	H	H	H	M	M	L	H	M	H	M	200
20.	Break wire	Walls, ceilings, floors	H	H	H	M	H	H	H	H	H	M	M	L	H	M	H	M	600

27A

TABLE 1. DEVICES, APPLICATIONS, AND EVALUATION (CONTINUED)

ITEM	DEVICE	APPLICATION	EVALUATION													
			EFFECTIVENESS					ENVIRONMENT					UTILITY		COST	
			Confidence that intrusion will be defeated	Resistance to defeat	Difficulty to observe	Operating reliability	Freedom from false alarms	Immunity to air turbulence	Immunity to noise (acoustic)	Immunity to noise (vibration)	Immunity to noise (electrical monochromatic)	Immunity to noise (electrical impulse)	Immunity to temperature changes	Ease of installation		Ease of calibration
21.	Break wire	Containers	H	L	H	M	H	H	H	H	H	M	L	H	M	\$ 200
22.	Chemical sniffer	Space	M	H	H	M	L	H	H	H	H	M	M	L	L	4,700
23.	Acoustic detector (microphone)	Windows, walls, ceilings, floors	M	L	L	M	L	M	L	M	H	H	M	L	M	400
24.	Acoustic detector (microphone)	Space	L	L	L	M	L	M	L	M	H	H	M	L	M	400
25.	Acoustic detector (microphone)	Containers	M	L	L	M	L	M	L	M	H	H	M	L	M	400
26.	Vibration detector	Windows, walls, ceilings, floors	M	L	L	M	M	H	H	L	H	H	M	L	M	400
27.	Vibration detector	Containers	M	L	L	H	M	H	H	L	H	H	M	L	M	400
28.	Thermal detector	Containers	M	L	M	M	H	H	H	H	H	H	M	H	M	400
29.	Acoustic motion low frequency	Space	H	H	L	H	M	M	H	H	H	H	M	L	M	450
30.	Acoustic motion ultrasonic	Space	H	H	L	M	L	L	M	M	H	H	M	L	M	500
31.	Microwave motion detector	Space	H	H	L	M	M	M	H	M	H	M	M	L	M	1,200
32.	Capacitive detector	Passageways	M	M	M	M	M	H	H	M	M	M	L	M	M	800
33.	Capacitive detector	Space	M	M	M	M	L	H	H	L	L	H	L	M	M	1,200
34.	Capacitive detector	Containers	H	M	M	H	M	H	H	H	H	M	M	H	M	450
35.	Strain gage	Windows, doors	M	M	H	H	H	H	H	M	H	H	M	H	M	350
36.	Strain gage	Walls, ceilings, floors	M	M	H	H	M	H	H	M	H	H	M	H	M	400
37.	Seismic	Floors	M	L	M	H	L	H	H	L	H	H	M	L	M	400
38.	Short or open line monitor	Communication lines	H	L	L	H	H	H	H	H	H	H	M	H	M	200
39.	Bridge line monitor	Communication lines	H	M	L	H	M	H	H	H	M	M	M	M	M	400
40.	Synchronous line monitor	Communication lines	H	M	L	M	H	H	H	H	M	M	M	M	M	1,200
41.	Cryptographic line monitor	Communication lines	H	H	L	M	H	H	H	H	H	H	M	M	L	2,000
42.	Secure transmission line	Communication lines	H	H	L	H	H	H	H	H	H	H	M	M	M	\$3.00/ft.

27B

ability of that product is substantially altered by the construction of the building; or area to be protected. Another equipment variable which makes it difficult to estimate costs, both from an acquisition and installation viewpoint, is that concerning control panels. Since most control panels vary in design, each has a different capability as to the number of detection devices which may be connected to and supervised by a single control panel. In view of obvious difficulties in computing acquisition and installation costs it is felt that general guidelines contained in paragraph c below will be of assistance.

c. The most practical and accurate way to obtain a cost estimate is to request two or more manufacturers to conduct an on-site survey and provide a cost estimate to the Government. This estimate is not to be considered by either party, the manufacturer or USATECOM as constituting a competitive bid which will take place later upon an Invitation for Bid. If a manufacturer will not conduct an on-site survey to provide the necessary information on which to base a cost estimate, "ball park" estimates may be obtained by providing the manufacturer with a written description of the area or areas to be protected. Such descriptions should include the following:

(1) A detailed scale drawing showing the intrusion detection system plan, to include the location of the area or areas to be protected, how they are to be zoned, and their relationships to master and local points in terms of distance.

(2) A scaled diagram of the area concerned, with a full description of the construction of the structures involved, to include the location of windows and doors; wall, floor, and ceiling construction; height of walls; partitions within the structure; operational equipment contained therein, such as motors, fans, blowers, air-conditioning, etc.; and the ambient noise level, if known.

(3) The type of system desired.

(4) Standards for equipment should be based upon the current Interim Federal Specification for Alarm Systems (Security) attached at Appendix C. Also attached at Appendix D are draft guideline specifications which are expected to become a part of the new OPMG Technical Bulletin on Intrusion Detection Alarm Systems.

(5) Other technical considerations which would effect the installation, operation and maintenance of the system(s) desired.

d. Draft guideline specifications are for USATECOM internal use only and will not be released to manufacturers or sales personnel for intrusion detection alarm systems.

CHAPTER IV
OPERATING AND MAINTAINING INTRUSION DETECTION ALARM SYSTEMS

1. Control Points.

a. Under normal conditions, at relatively small installations and activities, control panels will be located at the police headquarters where the desk or radio attendant may also monitor the control panels. This is called a master control point. At large installations or in extremely sensitive areas it will in most instances be desirable to establish control points in close proximity to the area under surveillance. These are termed local control points. Their primary purposes are to negate the distance between the police headquarters and the area under the detection system and reduce the cost and maintenance of the system. When feasible, local control point panels should have a parallel reporting line to the master control point. When this line is used it is not necessary to show which specific detection device has been alarmed, only which area has sounded the alarm. The purpose of this line is to preclude the neutralization of the local control point and to place the headquarters on immediate alert that an intrusion attempt is being made. Where a reporting line from local control points to a master control point is not feasible, some other similar system of alarm should be provided.

b. As a minimum, control points should:

- (1) Be located within security guard force headquarters.
- (2) Contain the control panels for all protected areas.
- (3) Be designated and posted as "sensitive areas," with access limited to authorized personnel only.
- (4) Be attended and operated by a member of the security police force during all hours the intrusion detection system is in operation.
- (5) Be adequately secured when not attended.
- (6) Be attended by a member of the guard force who has been specially trained in the operation of all electronic equipment located therein. (In the interests of economy, the attendant could be a member of the police force who is responsible for the operation of the police force communications system.)
- (7) Be inspected and operationally tested at least twice during each shift during the protected period.
- (8) Where feasible, contain a control panel from each local point.

2. Response Factors and Backup Protection.

a. In order to investigate the cause of an intrusion alarm it is necessary for police to respond to the area. Detection devices are capable only of indicating something is wrong in the protected area; therefore, security police must respond to the site of the alarm to investigate and neutralize the situation. The guard attending the control point normally cannot answer an alarm, as he should not leave his post. He must relay the information to other policemen for investigation. Areas of sufficient importance to be protected with intrusion alarm systems will normally be under police patrol as well. The guard on patrol should respond to the site of an alarm and investigate the cause.

b. It is an established security policy that one man should not answer the alarm alone. Simultaneous with the alarm, a backup force should be dispatched to the area under attack. The size of the backup force depends upon factors at each installation or activity. This manual will not attempt to prescribe the size or composition of a backup force, but will only recommend that one be in existence. Post assignments and moving patrol routes should be reviewed and modified if necessary, to provide backup forces which can respond within a maximum period of 15 minutes. This manual will not be used as a basis to create a reserve force for backup purposes in civilian guard forces. Where military police are used, this is normal practice, and no prohibition to this practice is intended by the preceding sentence.

c. Second in importance only to immediate response are the communications facilities connected with the intrusion detection system. Certain types of detection units either have, or may be modified to use, talk-back and listening features. These units allow instant communication with any or all areas under that particular control panel (unless they are wired directly in zones). They further allow the policeman on the control panel to monitor the response. Radio and telephones are alternate methods of communication which are usually available. When possible, radio contact and telephone lines to civil police agencies are desirable over and above intra-installation communications. Any plans for sealing off an area will involve communications. For the reasons outlined above, the following are suggested minimum communications requirements for control points.

(1) Two-way radio communications with motor patrols, police headquarters, and fixed posts.

(2) Telephone connections to all fixed posts and guard force headquarters.

(3) If no talk-back and listening features are built into the detection system, two-way radio communications with foot patrols in that area through use of portable radio equipment are essential.

3. Day-Night Control. The "day-night" control permits turning the protection system off so that authorized personnel may enter the protected area without causing an alarm. The guard must be previously alerted that authorized personnel are to enter the area, or some form of pre-arranged code signal must be transmitted to the guard station prior to entry, so that he may turn the alarm detectors off, and when the protected area is clear, restore protection. Some communication, either by code or voice, should be effected with the guard so as to positively establish departure by authorized personnel and insure that the protection system is operating, and that the guard has assumed responsibility for the protected area. Additionally this control should provide 24 hour reporting line supervision to detect tampering while in the "day" or "off" position.

4. False Alarms. An occasional false alarm is almost necessary to insure that the detection system is working. When no false alarms are sounded, the system should be checked to determine whether the settings are too insensitive or if it is actually in operation. Too frequent alarms, however, tend to develop laxity in response. No attempt will be made to establish a frequency ratio for false alarms; however, as a rule a system which creates more than one per week should be checked for oversensitivity or malfunction. When dissimilar systems for perimeter and interior protection are used, any simultaneous or closely connected alarms from both systems is an almost positive indication of an intrusion attempt. A clever agent or felon can easily time intrusion attempts to correlate with natural phenomenon such as thunder, snow, etc., which will tend to create a false alarm and thereby pass through the system under the guise of a false alarm.

5. Maintenance of Systems. Although the essentiality of continued operation of intrusion detection systems is a foregone conclusion, the maintenance of such systems is not a serious or difficult problem, particularly since the devices employed in these systems operate on electrical and radio principles. Since most installations have the personnel to maintain radio communications equipment, such personnel can also maintain intrusion detection equipment. In those cases where installation personnel are not available to maintain such equipment, service contracts can be entered into with the manufacturer, or with local service organizations if the manufacturer does not provide maintenance service. Most manufacturers are willing to train or advise installation personnel in the functioning and servicing of their equipment. The following minimum standards pertaining to installation and maintenance should be adhered to:

a. Drawings, plans, and/or diagrams of intrusion detection systems as pertains to electrical circuitry and location of detection devices, reporting lines, control panels, and any other technical details relating to the installation and operation of the system will be appropriately classified.

b. An adequate supply of reserve component parts (such as tubes, transistors, condensers, relays, etc.) should be maintained on hand to facilitate emergency repair of equipment. At those installations and activities where several detection systems are employed or where many control panels and detection devices are used, it is recommended that spare detection devices and control panels be obtained to provide for unit replacement of these devices and panels when required. Thus, a spare panel or detection device may be substituted for a defective one, thereby reducing the inoperative period of the system to a minimum.

c. An emergency kit containing component parts (such as tubes, transistors, relays, condensers, magnetic switches, etc) will be prepared and maintained at the master control point or maintenance shop in readiness for the immediate use of maintenance personnel when the system fails.

d. At 90-day intervals, in-place checks should be made on all equipment, with particular emphasis on tubes. Tubes determined to be functioning at less than 70-percent efficiency should be replaced.

6. Operational Records. After an intrusion detection system has been installed and is in operating condition, it is necessary to know something about its operating characteristics, for most systems will develop certain operating peculiarities, just as will occur in motor vehicles or other man-made appliances. Consequently, daily operating records should be maintained to analyze operating costs, replacement parts forecasting, alarm causes, effects of weather conditions, repeated malfunctioning of system's components parts, etc. This operational record should contain the following information:

- a. Date and time an alarm is received.
- b. Identity of the area from which the alarm signal was received.
- c. The identity of the person recording the alarm signal.
- d. The identity of the personnel and the time they were dispatched to the site of the alarm signal.
- e. The total elapsed time required for responding personnel to arrive at the site of the alarm signal.
- f. Cause of the alarm signal. Indicate whether it was caused by an intruder or by a defective component, loss of power, weather conditions, etc. When it has been determined that an intruder caused an alarm, the full details should be recorded on the security police operations journal, police blotter, or whatever system the guard force employs to record events. In the event the cause of the alarm cannot be determined,

the cause should be listed as "unknown." If the cause of the alarm was due to a defect in the system, record the length of time the system was inoperative and the date, time, and identity of the person repairing same.

APPENDIX A

LIST OF MANUFACTURERS

(INTRUSION DETECTION

ALARM SYSTEMS)

LIST OF MANUFACTURERS

Manufacturer

Code Letter
(Ref Appendix B)

Advanced Devices Laboratory, Incorporated
701 Kings Row
San Jose, California

A

Air Space Devices, Incorporated
Dept. P-11, PO Box 338
Paramount, California 90723

B

Alarmatronics Engineering, Incorporated
154 California Street
Newton, Massachusetts 02195

C

American District Telegraph Company
155 Sixth Avenue
New York, New York 10013

D

American Sentry Sales Corporation
67 Van Nuys Boulevard
Van Nuys, California 91403

E

Arrowhead Enterprises, Inc.
Route 6
Bethel, Connecticut 06801

F

Auricord Division, Scovill
35-41 29th Street
Long Island City, New York 11106

G

Autocom Division
General Research Corporation
75 Rowe Street
Newton, Massachusetts 02166

H

Automatic Protection Systems Division
of "Automatic Sprinkler" Corp. of America
7809 Market Street
PO Box 24207
Houston, Texas 77029

I

Automatic Telemetry Devices, Inc.
A Subsidiary of Schick Electric, Inc.
11704 Wilshire Boulevard
Los Angeles, California 90025

J

List of Manufacturers (Continued)

Manufacturer

Code Letter
(Ref Appendix B)

Bagno Alertronics, Inc.
A Subsidiary of Systron Donner
135 Main Street
Belleville, New Jersey

K

Barnes Engineering Company
30 Commerce Road
Stanford, Connecticut

L

Continental Telephone Supply
17 West 46th Street
New York, New York 10036

M

Control and Communications, Inc.
301 Main Street
Festus, Missouri 63028

N

Defensive Instruments, Inc.
9 Penn Avenue
Pittsburgh, Pennsylvania 15222

O

Detection Systems, Inc.
211 Eyer Building
East Rochester, New York 14445

P

Devenco Incorporated
Research and Development Division
150 Broadway
New York, New York 10038

Q

Digital Identification Systems
9200 Glendaks Boulevard
Sun Valley, California 91352

R

Electroprotective Devices, Inc.
1767-A Wilson Avenue
Chicago, Illinois 60640

S

Electrosystems Corporation
3954 N. E. 5th Avenue
Fort Lauderdale, Florida

T

Engarde Corporation
131 N. Main Street
Gates, California

U

Euphonics Corporation
202 Park Street
Miami Springs, Florida 33166

V

List of Manufacturers (Continued)

Manufacturer

Code Letter
(Ref Appendix B)

A. W. Fruh and Company
1817 Orchard Street
Chicago, Illinois 60614 W

GBC Closed Circuit TV Corporation
74 Fifth Avenue
New York, New York 10111 X

General Electric Company
1 River Road
Schenectady, New York 12305 Y

General Systems Industries, Incorporated
Del Amo Financial Center
Torrance, California 90503 Z

G-R Industries, Inc.
76 Rowe Street
Newton, Massachusetts 02116 AA

Guard Alarms
1771 Wilson Avenue
Chicago, Illinois 60640 AB

Guardian Electronic Systems, Inc.
3342 Saw Mill Run Blvd.
Pittsburgh, Pennsylvania 15227 AC

Honeywell
Commercial Division
2701-4th Avenue, So.
Minneapolis, Minnesota 55408 AD

Imperial Products Co.
37-08 Greenpoint Avenue
Long Island City, New York 10001 AE

I. Tronics Division
International Assembly Corporation
2101 Auburn Avenue
Toledo, Ohio 43606 AF

Jackson and Church Electronics
Eau Gallie, Florida AG

Johnson Service Company
507 E. Michigan Street
Milwaukee, Wisconsin 53201 AH

List of Manufacturers (Continued)

Manufacturer

Code Letter
(Ref Appendix B)
AI

Kelpak Systems Inc.
PO Box 64764
Los Angeles, California 90064

AJ

Laser Systems Corporation
313 N. First Street
Ann Arbor, Michigan 48103

AK

Lectro Systems Inc.
1245 Pierce Butler Route
St. Paul, Minnesota 55104

AL

Linear Corporation
347 S. Glasgow
Inglewood, California 90301

AM

Melpar, Incorporated
3000 Arlington Boulevard
Falls Church, Virginia 22041

AN

Microwave and Electronics Systems, Ltd.
Security Electronics
11 E. 43rd Street
New York, New York 10017

AO

Minitrox Systems Corporation
Empire State Building
New York, New York 10001

AP

Mithras Division
Sanders Associates, Inc.
701 Concord Avenue
Cambridge, Massachusetts 02138

AQ

Mosler Research Products, Inc.
9 South Street
Danbury, Connecticut 06810

AR

Normda Industries, Inc.
PO Box 20024
San Diego, California 92120

AS

Notifier Company
3700 North 56th Street
Lincoln, Nebraska 68504

AT

Orinerton's Inc.
20 N. Wacker Drive
Chicago, Illinois 60606

List of Manufacturers (Continued)

Manufacturer

Code Letter
(Ref Appendix E)

Radar Detection Systems, Inc.
6300 Northern Boulevard
East Norwich, New York 11732

AU

Radar Devices Manufacturing Company
22003 Harper Avenue
St. Clair Shores, Michigan 48080

AV

Radion Corporation
6900 S. State Road 84
Fort Lauderdale, Florida 33314

AW

Santa Barbara Research Center
75 Coromar Drive
Goleta, California 93017

AX

Schulmerich Electronics, Inc.
Carillon Hill
Sellersville, Pennsylvania 18960

AY

Security Devices Associates
156 Fifth Avenue
New York, New York 10010

AZ

Security Electronics, Inc.
Box 14224
Omaha, Nebraska 68114

BA

Security Systems of America
A Division of the Convento Company
51st and A. V. R. R.
Pittsburgh, Pennsylvania 15201

BB

Singer-Bridgeport
915 Pembroke Street
Bridgeport, Connecticut 06608

BC

Solid State Research Corporation
640 Coors Road, S. W.
Albuquerque, New Mexico 87105

BD

Sonaguard, A Division of Sentron, Inc.
119 Dover Street
Somerville, Massachusetts 02144

BE

List of Manufacturers (Continued)

Manufacturers

Code Letter
(Ref Appendix B)

Space Age Mfg. Co., Inc.
7118 Canby Street
Reseda, California 91355

BF

Sylvania Electronic Products
Security Systems Division
Mountain View, California 94040

BG

Squires Sanders Incorporated
Martinsville Road
Liberty Corner, New Jersey 07938

BH

Texas Instruments
Science Services Division
6000 Lemmon Avenue
Dallas, Texas 75209

BI

Walter Kidde and Company
Lenville, New Jersey 07109

BJ

Westinghouse Electric Corporation
Security and Solid States Systems Department
PO Box 8606
Pittsburgh, Pennsylvania 15221

BK

APPENDIX B

INTRUSION DETECTION ALARM SYSTEM

IDENTIFICATION AND EVALUATION

W. H. Helms

APPENDIX C

INTERIM FEDERAL SPECIFICATION

ALARM SYSTEMS, PROTECTIVE, INTERIOR

(SECURITY)

INTERIM FEDERAL SPECIFICATION
ALARM SYSTEMS, INTERIOR, SECURITY,
COMPONENTS FOR

This Interim Federal Specification was developed by Standardization Division, Federal Supply Service, General Services Administration, Washington, D. C. 20406, based upon currently available technical information. It is recommended that Federal agencies use this document in procurement and forward any recommendation for changes to the preparing activity at the address shown above.

1. SCOPE AND CLASSIFICATION

1.1 Scope. This specification covers a group of units which, when selectively assembled, provide interior alarm systems specifically designed for security applications (see 6.1). These properly assembled systems are highly resistant to neutralization or compromise by covert or surreptitious attack.

1.2 Classification.

1.2.1 Units. Products furnished under this specification shall consist of the following units, as specified (see 6.2).

- Unit 1 - Detector (see 3.3).
- Unit 2 - Annunciator (see 3.4).
- Unit 3 - Supervisory circuit (see 3.5).

1.2.2 Detectors. Detectors furnished under this specification shall be of the following types, as specified (see 6.2).

- Type I - Approach detector (doors, windows, ducts, and wall devices).
- Type II - Linear detector (photoelectric, infra-red, and similar light devices).
- Type III - Surface detector (sound and vibration devices).
- Type IV - Volumetric detector (electromagnetic and other motion sensing devices).

1.2.3 Alarm transmission means. The alarm transmission means (supervisory circuits) furnished under this specification shall be of the following classes, as specified (see 6.2).

- Class A - Wire transmitted (see 3.5.1).
- Class B - Radio transmitted (see 3.5.1).

2. APPLICABLE DOCUMENTS

2.1 The following documents of the issues in effect on the date of invitation for bids or request for proposal, form a part of this specification to the extent specified herein:

Federal Standard:

Fed. Std. No. 123 - Marking for Domestic Shipment (Civilian agencies)

(Activities outside the Federal Government may obtain copies of Federal Specifications, Standards, and Handbooks as outlined under General Information in the Index of Federal Specifications and Standards and at the prices indicated in the Index. The Index, which includes cumulative monthly supplements as issued, is for sale on a subscription basis by the Superintendent of Documents, U. S. Government Printing Office, Washington, D. C. 20402.

(Single copies of this specification and other Federal Specifications required by activities outside the Federal Government for bidding purposes are available without charge from Business Service Centers at the General Services Administration Regional Offices in Boston, New York, Washington, D.C., Atlanta, Chicago, Kansas City, Mo., Fort Worth, Denver, San Francisco, Los Angeles, and Seattle, Washington.

(Federal Government activities may obtain copies of Federal Specifications, Standards, and Handbooks and the Index of Federal Specifications and Standards from established distribution points in their agencies.)

Military Specifications:

- MIL-T-6807 - Tests, Vibration and Shock, Ground Electronic Equipment, General Requirement for
- MIL-E-17555 - Electronic and Electrical Equipment and Associated Repair Parts, Preparation for Delivery Of

(Copies of Military Specifications and Standards required by contractors in connection with specification procurement functions should be obtained from the procuring activity or as directed by the contracting officer.)

2.2 Other publications. The following documents form a part of this specification to the extent specified herein. Unless a specific issue is identified, the issue in effect on date of invitation for bids or request for proposal shall apply.

American National Standards Institute (ANSI) Inc. Standards:

- C39.1 - Electrical Indicating Instruments, (Panel, Switchboard, and Portable Instruments), Requirement for

(Applications for copies should be addressed to the American National Standards Institute, 1430 Broadway, New York, N.Y. 10018.)

3. REQUIREMENTS

3.1 Qualification. The alarm system units furnished under this specification shall be products which have been tested, and passed the qualification tests specified in section 4, and have been listed on or approved for listing on the applicable Federal Qualified Products List (QPL).

3.1.1 Listing of Alarm system components. To have alarm system units listed on the applicable QPL shall require the testing and approving of a group of components of the type the manufacturer proposes to furnish, to include a detector specified in 3.3, an annunciator specified in 3.4, a transmission means or supervisory circuit specified in 3.5, which may or may not be integral with the annunciator, a power supply specified in 3.6, and other parts and circuits required for a complete working system. The components, when approved, will be listed on the applicable QPL as individual items.

3.2 Parts and materials. Parts and materials for components shall be as specified herein. Those not definitely specified shall be equivalent to and interchangeable with the corresponding part, material, or process in the manufacturer's normal commercial product. Normal commercial product shall be interpreted to mean an end item covered by this specification.

3.2.1 Panel and mounting racks. Panels and racks shall be in accordance with ANSI Standard C39.1. All soldered connections shall be mechanically secured before soldering.

3.2.2 Boxes and cases. All terminal, junction, and utility boxes, switch cases, and similar receptacles shall be protected against tampering and in each instance, the enclosures shall be equipped with inter-lock switches or triggering mechanisms electrically compatible with the alarm system; or shall be fully filled with an epoxy compound to preclude tampering. In both day (access) and night (secure) modes of operation, all components of the system shall be continuously circuit supervised to preclude the unauthorized removal of a component without activation of an alarm.

3.3 Detectors. The detectors shall provide an alarm response under any of the following conditions: (1) A penetration of the protected area; (2) A failure in the detector's power source; (3) Any malfunction which affects the detector's ability to function properly. The sensitivity and stability of the detectors shall be such as to preclude nuisance alarms. Terminals shall be accessible to permit wiring for required combinations of detection units. All controls necessary for operator use shall be located for maximum accessibility and minimum accidental change, and marked for easy recognition. All controls and terminals which are not required for the operation of the alarm system shall not be readily accessible to the operator.

3.3.1 Approach detector (type I). The type I detector shall create an alarm response when an electrical current is interrupted or altered. Such interruption or alteration may be created by breaking a circuit wire or foil strip, by shorting a circuit, by opening a switch, or by changing an electrical resistance. Foil wire, and switches shall be as specified hereunder.

3.3.1.1 Protective foil. Protective foil used shall not exceed 1.2 pounds tensile strength and shall be capable of carrying a minimum current of 60 milliamperes at 60 volts with a temperature rise of not more than one degree centigrade. Foil shall be provided in 1/2-inch and 1 inch widths.

3.3.1.2 Protective wire. Protective wire used in fabricating security screens shall not exceed 4.0 pounds tensile strength, and shall be capable of carrying a maximum current of 60 milliamperes at 60 volts with a temperature rise of not more than one degree centigrade. Wire shall be not larger than 30 AWG, and shall be firmly fastened in grooves at intervals of not more than 18 inches and in such a manner that removal from the grooves shall not be possible without breaking the wire or damaging the groove material. Wiring shall be continuous without splices from one connecting point to another.

3.3.1.3 Movable opening switches. Movable opening switches shall be capable of withstanding 50,000 activations without affecting serviceability and shall be electrically connected so that mechanical activation of switches results in an open circuit followed by a short or closed circuit which creates an alarm response. These switches shall be designed so that they can be securely mounted to permanent structure such as doors and door and window frames.

3.3.1.4 Magnetic switches. These switches shall be completely enclosed and shall not be susceptible to defeat by the application of an external magnetic source.

3.3.1.5 Mechanical switches. Mechanical switches shall be single-pole, double-throw, and completely enclosed.

3.3.1.6 Mercury switches. Mercury switches shall be completely enclosed and the mercury and contacts shall be contained in a hermetically sealed tube.

3.3.2 Linear detector (type II). The type II detector shall create an alarm response by a change of 10 percent or more in the modulated character of the light beam, or by the passing of a person through the field, beam, or antenna array along the protected perimeter.

3.3.2.1 Modulated light beam. The modulated light beam for the type II detector shall not be visible to the unaided eye. Shielding shall be provided so that the light source is not visible when viewed at an angle of fifteen degrees from the axis of the beam.

3.3.3 Surface detector (type III). The type III detector shall create an alarm response as a result of the sound level in the protected area rising four decibels above the ambient level in 10 seconds or less, or by the approach of a person to within six inches of a protected object.

3.3.4 Volumetric detector (type IV). The type IV detector shall create an alarm response as the result of a disturbance to an energy field in a defined space, such as the motion of a person walking not more than four steps at a rate of one step per second followed by a three-second pause anywhere in the space protected.

3.3.4.1 Neutralization of type IV detectors. The type IV detectors shall not be susceptible to defeat by the introduction of micro-wave or other radiated energy absorptive or reflective materials, or by saturation or neutralization from external oscillator sources.

3.4 Annunciators.

3.4.1 Annunciator capability. The annunciator shall physically and electrically match and connect with other components in the alarm system and shall be capable of indicating by colored signal lights the following system conditions: (1) That normal system conditions exist (green light); (2) That a detector in a protected area is in alarm condition, or that power failure or malfunction of a component has caused the alarm system to be inoperative (red light); (3) That the annunciator is operating on standby power (yellow light).

3.4.2 Annunciator response devices. The annunciator shall contain both visible and audible signalling devices in redundancy which will respond to changes in line signal (see 3.5.1).

3.4.3 Annunciator alarm and reset conditions. An alarm shall create a lock-in condition which shall require manual restoration, and controls shall be provided to reset the system. The annunciator shall have a means to silence the audible signal from a particular zone during prolonged alarms. However, the visible signal shall remain indicated on the annunciator panel until the system is restored to normal operation. The silencing control shall be so connected that the audible alarm signal will be activated upon receipt of each alarm. During the periods when the alarm system is not in active operation and the detectors in the protected areas are officially desensitized, the annunciator shall continue to detect the same changes in normal line current or tampering with the system as required during the periods of active operation.

3.4.4 Installation and mounting. Where the installation consists of one to four annunciators, the equipment shall be designed to allow stacking, rack mounting, or the use of modular construction. Where the installation consists of five or more annunciators, the equipment shall employ rack mounting or modular construction. To the extent practicable, equipment related to the operation of the annunciators shall be contained in one housing. Individual annunciators of a given manufacturer shall be interchangeable to facilitate maintenance. Plugs and sockets shall be used where possible. All parts of the annunciator shall be easily identified and readily accessible to authorized maintenance personnel to facilitate official repair and inspection. All controls required for normal operation shall be conspicuously marked and located to provide maximum access and minimum accidental change. All controls not required for operation shall be inaccessible to the operator.

3.4.5 Connection of annunciators to power sources and transmission lines. Inter-connections between the supplied power and the annunciator shall be made within the annunciator housing. A multiple terminal cross-connection block shall be provided within the annunciator housing when 4 or more annunciators require joint use.

3.4.6 Maximum line current and voltage. Alternating or direct current from transmission lines into annunciators shall not exceed 30 milliamperes. Alternating or direct voltages, or alternating voltages superimposed on direct voltages into annunciators shall not exceed 100 volts.

3.5 Transmission means (Supervisory circuit). The supervisory circuit shall be resistive to neutralization or compromise and shall provide security to the communication link between the detector and the annunciator. The circuit shall consist of a distal unit which connects to the detector, and receives therefrom the initial alarm signal, and the proximal unit which connects to the annunciator and provides it with the signal to initiate the final alarm response. The supervisory circuit shall use the same type of power as the detector and annunciator. All controls and switches which are for operator use shall be located for maximum accessibility and minimum accidental change, and marked for easy recognition. All controls which are not required for operation of the system shall not be accessible to the system operator.

3.5.1 Classes.

Class A - The class A supervisory circuit shall provide an alarm response in the annunciator as a result of the following changes in the normal transmission line current.

- (1) Five percent or more in normal line signal when it consists of direct current from 0.5-milliamperes through 30 milliamperes.
- (2) Ten percent or more in normal line signal when it consists of direct current from 10 microamperes to 0.5-milliamperes.
- (3) Five percent or more in any component of the normal line signal when it consist of an alternating current of a frequency from one through one hundred cycles per second and 0.5-milliamperes through 30 milliamperes, and
- (4) Fifteen percent or more in any component of the normal line signal when it consist of an alternating current of a frequency higher than 100 cycles per second superimposed on a direct current having any value from 0.5-milliamperes through 30 milliamperes.

Class B - The class B supervisory circuit shall provide an alarm response to the annunciator as a result of an increase or decrease of at least 10 percent in the amplitude, frequency, or phase of the carrier signal used for the transmission of signal from the detection component.

3.5.2 Radiation interference. Operation of devices and annunciators shall not adversely affect radio transmission or reception in the vicinity in which operated.

3.6 Power supplies and sources.

3.6.1 Primary power. Primary power for alarm system components shall be public utility, battery, or other self generated sources.

3.6.2 Auxiliary power. An auxiliary power source for use in the event the primary source fails shall be provided by the manufacturer of the components submitted for qualification. The auxiliary power source shall be capable of maintaining full operation of the alarm system for not less than 72 hours. The auxiliary source shall be provided with a means to read or measure its potential at any time. A switch-over to auxiliary power shall be automatic upon failure of the primary power source. A signal shall be activated at the annunciator panel to indicate this condition.

3.6.3 Batteries. Batteries shall be rechargeable and shall have provisions to keep batteries fully charged or subject to automatic recharge whenever battery voltage drops ten percent below their normal rating. Recharge time shall not exceed 12 hours.

3.6.4 Voltage tolerance. A signal shall be registered at the annunciator panel if the voltage of the power source, primary or auxiliary, falls below 80 percent or exceeds 120 percent of normal when supplying power to the alarm system circuit. If the system is capable of normal operation at 50 percent of full voltage, the signal shall be registered at plus 50 percent or minus 50 percent of normal. Stable operation of the systems shall be maintained on both the primary and auxiliary power source within these variations.

3.6.5 Ventilation. Power supplies shall be vented or otherwise protected to preclude deterioration of any component parts.

3.7 Identification markings. A metallic plate or plates shall be affixed to detector and annunciator components specified in 1.2.1, which shall show the manufacturer's name, year manufactured, type and serial number, and the symbol "Int. Fed. Spec. W-A-00450A."

3.8 Technical manuals and operators instructions. Technical manuals and operators instructions containing complete and comprehensive instructions shall be furnished by the manufacturer. The manufacturer's literature shall be delivered with the alarm equipment. The manuals shall include schematics and wiring diagrams for all components and a complete electrical parts list fully identifying the parts and reflecting electrical values and ratings.

3.9 Workmanship. All components shall be manufactured and finished in such a manner as to meet specification requirements. Circuit wiring shall be neat with good electrical connections which are mechanically secure. Components and parts shall be free from characteristics and defects which might affect appearance or serviceability.

3.10 Spare parts. Spare parts as required by the procuring activity shall be furnished as specified (see 6.2).

4. QUALITY ASSURANCE PROVISIONS

4.1 Inspection responsibility. Except as otherwise specified herein, the supplier is responsible for the performance of all inspection requirements as specified herein. Except as otherwise specified, the supplier may utilize his own or any other inspection facility or services acceptable to the Government. Inspection records of the examinations and tests shall be kept complete and available to the Government as specified in the contract or order. The Government reserves the right to perform any of the inspections set forth in this specification where such inspections are deemed necessary to assure that supplies and services conform to prescribed requirements.

4.2 Component and material inspection. In accordance with 4.1, the supplier is responsible for insuring that components and materials used are manufactured, tested, and inspected in accordance with the requirements of referenced subsidiary specifications and standards to the extent specified, or, if none, in accordance with this specification.

4.3 Inspection for acceptance. Units to be offered for acceptance may be inspected by a Government inspector at any time during manufacturing processes to assure that the units function as intended, that parts and materials are complete and as specified, that parts and components are properly matched, that panels and racks are neatly wired, that junction and terminal points are properly located, that mechanical and electrically connections are secure, that soldered connections provide good electrical conductivity, that terminal boxes and switch cases are protected against tampering, and that all workmanship details are of good quality. When specified (see 6.2), acceptance inspection shall be performed at destination after equipment is installed ready for use.

4.3.1 Testing for acceptance. To assure continued compliance with specification requirements relating to operational performance, the Government reserves the right to select from the manufacturer's regular production, samples of alarm system components for testing in accordance with 4.6.1 through 4.6.7. The components selected shall constitute all units and parts necessary for a complete, working alarm system. The testing shall be performed by a facility designated by the Government and shall be at no cost to the manufacturer. Failure to meet testing requirements shall provide reason to suspend acceptance of the manufacturer's production until the Government inspector is satisfied that the manufacturer has corrected all defects in his products.

4.4 Inspection of preparation for delivery. An inspection of preparation for delivery shall be made in accordance with section 4 of MIL-E-17555.

4.5 Qualification. In accordance with 3.1, products submitted for qualification shall be inspected for workmanship as specified in 4.3 and subjected to the tests in 4.5.6.1 through 4.5.6.7. Failure to meet inspection or testing requirements shall be considered as failure to meet requirements for QPL approval.

4.5.1 Testing agency. Qualification testing shall be performed by a Government agency designated by the General Services Administration.

4.5.2 Testing costs. All costs entailed in testing the qualification samples shall be borne by the manufacturer and shall be payable to the General Services Administration as directed by the Standardization Division, Federal Supply Service.

4.5.3 Test sample. The samples submitted for qualification in accordance with 3.1 and 3.1.1 shall consist of all components necessary for a complete working alarm system of the type the supplier proposes to furnish. The samples' transportation fee prepaid, shall be forward at a time and to a place designated by Standardization Division, Federal Supply Services. In the event the product is approved for QPL, the test sample shall be retained by the Government during the term of qualification. Any sample not approved shall be returned to the manufacturer as is. Samples shall be identified by Tags, legibly marked as follows:

Sample for qualification under Int. Fed. Spec. W-A-00450A.
Type of component _____
Date of manufacture _____
Manufacturer's name and address _____
Location of manufacturer's plant _____

4.5.4 Technical manuals, diagrams and schematics. The manufacture shall furnish with the test sample a complete set of technical manuals, wiring diagrams, and schematics specified in 3.8 for use during the testing of the products for qualification.

4.6 Tests.

4.6.1 Performance tests. Samples submitted for qualification shall be assembled so as to provide a complete alarm system. The system shall then be tested to determine whether the component parts perform as intended under the various conditions specified in section 3. Detectors shall be tested for ability to provide an alarm response under the three conditions specified in 3.3. Annunciators shall be tested for ability to indicate the three alarm system conditions specified in 3.4.1, reflect changes in line signals as specified in 3.5.1, and comply with alarm and reset conditions specified in 3.4.3. Supervisory circuits shall be tested for ability to provide an alarm response as a result of changes in transmission line current (class A) or changes in carrier signal (class B) as specified in 3.5.1.

4.6.2 Neutralization or compromise tests. Tests shall be conducted to determine the ability of the supervisory circuit to protect the transmission line against neutralization or compromise. The tools and devices used in testing shall not exceed that equipment capable of being carried in two cases or containers, each case or container not to be more than 10 by 20 by 27 inches in size. Various methods of attack shall be made during the testing and any successful attack within the tool limitation specified shall be considered failure of the supervisory circuit to meet testing requirements.

4.6.3 Stability test. Alarm system sensitivity shall be tested to determine stability. This will be accomplished in a laboratory environment. The system components shall have their sensitivity controls set to meet the criteria set forth in section 3. Except during the testing of detection components, there shall be no alarm registered during a seven-day period of continuous operation. During the seven-day period, variations of the preset sensitivity of the system shall not exceed ± 5 percent.

4.6.4 High temperature test. Components for the system shall be placed in a high temperature chamber and the internal temperature of the chamber raised to 71 degrees centigrade (160°F.) for a period of 48 hours. The temperature shall then be reduced to prevailing room conditions and the components tested as specified in 4.6.1.

4.6.5 Low temperature. The components of the alarm system shall be placed in a low temperature chamber and the chamber cooled to and maintained at a temperature of minus 60 degrees centigrade (-80°F.) for a period of 72 hours. The temperature shall then be raised to prevailing room conditions and the items tested as specified in 4.6.1.

4.6.6 Humidity. The components of the alarm system shall be placed in a test chamber set up to simulate adverse humidity conditions. The test chamber shall be vented to the atmosphere to prevent the build-up of pressure and components will be protected from the dripping of moisture. Prior to the start of the test period, the chamber temperature shall be between 20 degrees centigrade and 38 degrees centigrade (68°F. and 100°F.) with uncontrolled humidity. During the first 2-hour period, the temperature shall be gradually raised to 50 degrees centigrade (122°F.). This temperature shall be maintained during the next 6-hour period. The velocity of the air throughout the test area shall not exceed 150 feet per minute. During the following 16-hour period, the temperature in the chamber shall be gradually reduced to between 20 degrees centigrade and 38 degrees centigrade (68°F. and 100°F.) which shall constitute one cycle. The relative humidity throughout the cycle shall be at least 95 percent. Steam or distilled water having a pH value between 6.5 and 7.5 at 25 degrees centigrade (77°F.) shall be used to obtain the desired humidity. The cycle shall be repeated a sufficient number of times to extend the total time of the test to 240 hours (10 continuous cycles). At the conclusion of the 240-hour period, the equipment shall be returned to prevailing room conditions, and moisture removed from the components by turning or wiping them without disassembly or the application of heat or air blast. As soon as possible after completion of the 240-hour period the items shall be tested as specified in 4.6.1.

4.6.7 Vibration test. Alarm components shall be subjected to the applicable vibration test in MIL-T-4807.

5. PREPARATION FOR DELIVERY

5.1 Preservation, packaging, packing and marking shall be in accordance with MIL-E-17555. The level of preservation and packaging shall be A or C, and the level of packing shall be A, B, or C as specified (see 6.2).

5.1.1 Civil agency marking. In addition to any special marking (see 6.2) required by the contract or order, the interior packages and shipping containers shall be marked in accordance with Fed. Std. No. 123.

6. NOTES

6.1 Intended use. Alarm systems constructed with components qualified and approved under the requirements of this specification are intended to supplement or support guard systems for areas housing classified materials or activities as determined by the responsible authority.

6.2 Ordering data. Purchaser should exercise any desired options offered herein, and procurement documents should specify the following:

- (a) Title, symbol, and date of this specification.
- (b) Type of detector and number required (see 1.2.2).
- (c) Number of annunciators required (see 1.2.1).
- (d) Class of transmission means required (see 1.2.3).
- (e) Spare parts required (see 3.10).
- (f) Destination inspection required (see 4.3).
- (g) Selection of applicable levels of packaging, packing, and marking (see 5.1).
- (h) Any special marking required (see 5.1.1).

b.3 Qualification. With respect to products requiring qualification, awards will be made only for such products as have, prior to the time set for opening of bids, been tested and approved for inclusion on the applicable Federal Qualified Products List, whether or not such products have actually been so listed by that date. The attention of suppliers is called to this requirement, and manufacturers are urged to arrange to have the products they propose to offer to the Federal Government tested for qualification so that they may be eligible to be awarded contracts or orders for the products covered by this specification. The activity responsible for the Qualified Products List is Standardization Division, Federal Supply Service, General Services Administration, Washington, D.C. 20406, and information pertaining to qualification may be obtained from that activity.

GENERAL SERVICES ADMINISTRATION - FEDERAL SUPPLY SERVICE
SPECIFICATION COMMENT SHEET

BUDGET BUREAU NO.
29-R0175

INSTRUCTIONS

This form provides a way for users of this specification to inform the originator of problems encountered in its use. It is not to be used to request changes to accommodate proprietary features. All comments will be considered and appreciated, but please do not expect a reply. To comment: detach, complete, fold, staple, and mail.

NOTE: Comments on this form do not constitute or imply authorization to waive any part of the document or serve to amend contractual requirements.

1. SPECIFICATION

W-A-00450A (GSA-FSS) Alarm Systems, Interior, Security, Components For

2. CONTRACT NO. (If any)

3. QUANTITY ON CONTRACT (Optional)

4. DOLLAR VALUE (Optional)

5. GENERAL NATURE OF PROBLEM (e.g., inspection difficulties, manufacturers unable to meet tolerances, containers collapse under normal warehousing conditions, etc.)

6. SPECIFIC REQUIREMENTS AFFECTED (Include paragraph number and lines of wording)

7. SPECIFIC PROBLEMS (e.g. tests in 4.2.2 will not assure that the battery will last required time; temperature ranges in table 2 do not conform to commercially available items.)

8. RECOMMENDATIONS

9. NAME OF MANUFACTURER, ASSOCIATION, GOVT., AGENCY, ETC.

10. ADDRESS (Number, Street, City, State and Zip Code)

11. NAME AND TITLE OF SUBMITTER

12. DATE

FOLD

GENERAL SERVICES ADMINISTRATION

OFFICIAL BUSINESS



POSTAGE & FEES PAID
GENERAL SERVICES ADMINISTRATION

General Services Administration
Federal Supply Service (FMSO)
Washington, D. C. 20406

FOLD

APPENDIX D

(REVISED)

CTPMG GUIDELINE SPECIFICATIONS

INTRUSION DETECTION ALARM SYSTEMS

FOR OFFICIAL USE ONLY

PHYSICAL SECURITY

OFFICE OF THE PROVOST MARSHAL GENERAL

DA STANDARDS

INTERIOR

INTRUSION DETECTION EQUIPMENT

FOR

PHYSICAL SECURITY APPLICATION

FOR OFFICIAL USE ONLY



DEPARTMENT OF THE ARMY
OFFICE OF THE PROVOST MARSHAL GENERAL
WASHINGTON, D.C. 20314

PREFACE

It is impractical to prescribe definitive Department of Army physical security standards to cover all anticipated conditions which pose a threat to the security of government property, since the estimated degree and nature of the threat are contingent upon many variables which often are not constant. It is imperative, therefore, that local physical security personnel, through a continuous local threat assessment, and periodic physical security surveys and inspections, insure the application of required measures to protect government property, to include application of interior intrusion detection systems.

The use of intrusion detection equipment has proven, in many instances, to provide a valuable adjunct to the local security program. Such equipment, however, is not a panacea for security problems and if not understood or misused, may actually aggravate an already tenuous security situation. It is, therefore, necessary for potential users of such equipment to understand the basic theory of operation, equipment capabilities and limitations, equipment selection process, Department of Army standards for interior-intrusion detection equipment, the procurement process in obtaining such items, and considerations regarding installation and maintenance. This document is intended to provide that information.

Lloyd B. Ramsey
LOYD B. RAMSEY
Major General, USA

The Provost Marshal General

TABLE OF CONTENTS

SECTION		PAGE
I	Intrusion Detection Systems (General	1
	Introduction	1
	Definitions	2
II	Type of Systems	6
	General	6
	Equipment Application	14
III	Facility Survey	15
IV	Standards for Interior Intrusion Detection Equipment	25
V	Standards for Installation of Interior Intrusion Detection Systems	57
VI	Standards for Preventative Maintenance and Emergency Service	64
VII	Procurement of Intrusion Detection Systems	69
VIII	Qualified Intrusion Detection Equipment	75

APPENDIX

- A. Facility Survey Checklist
- B. Procurement Package Outline

SECTION I

INTRUSION DETECTION SYSTEMS

General

A. Introduction

1. Intrusion Detection Equipment (ID) is employed for the purpose of detecting and announcing proximity or intrusion which endanger or may endanger the security of protected property or areas.

2. Intrusion Detection systems are utilized to accomplish one or more of the following objectives:

a. To permit more economical and efficient use of manpower by substitution of mobile responding guard units for larger numbers of fixed guards and/or patrols.

b. To substitute for other structural measures normally used in the physical security posture when the building layout, safety regulations, operating requests, appearance, cost or for other reasons, make the use of ID systems more practical.

c. To provide additional controls at vital areas as insurance against human or mechanical failure.

3. One of the primary considerations in the application of ID equipment is the ability of a designated security force to rapidly respond to an alarm received at a central location. To be effective, a security force must be capable of responding to an alarm within a maximum of ten minutes. Exception to this principle is when the system is being used primarily as a psychological barrier to deter would-be criminal elements with the chance response to the alarm by personnel in the area at the time.

4. An intrusion detection system is usually made up of three component parts.

a. First, the sensing or detection device. This is the component which detects the situation for which it was designed. It initiates the signal that will ultimately provide the alarm.

b. The monitoring device. The device that receives the alarm signal and converts it into a usable response designed to ultimately correct or allow correction of the undesirable situation which has been detected.

c. The transmission System. This component transmits or transfers the initial signal from the detection to the location at which the alarm is sounded.

B. Definitions: The following definitions are provided as an aid in understanding both the construction and operation of ID equipment:

1. Alarm - A signal generated when detection equipment within the protected area responds to the presence of a condition that it is designed to detect.
2. Alarm, False - Signal caused by a factor other than an actual alarm.
3. Annunciator - Same as monitor panel.
4. Cabinet, Monitor - The enclosure which houses the monitor panels and associated equipment.
5. Connect Police - Lines connected to a monitor in the local police station in addition to the connection in the proprietary monitor or central station monitor.
6. Contact - Same as door switch.
7. Control, Access/Secure - Control used with constantly supervised security systems to allow normal traffic through a protected area during the hours of occupancy. This control renders the system inoperative but allows tamper and line supervision to be maintained to prevent the system from being compromised during the hours of normal occupancy.

8. Control, Permitt - Same as access/secure control.
9. Detector - Any device which senses the presence of an intruder and causes an alarm to be generated.
10. Detector, Capacitance - A device which detects the approach to or touching of a protected object such as a safe, filing cabinet, or capacitance grids protecting windows, air conditioning, ducts, or other openings in the perimeter of a protected area. This detection senses a change in the capacitance caused by an approaching mass and causes an alarm to be generated.
11. Detector, Infrared - Photo-electric intrusion detection device which uses infrared light rather than visible light.
12. Detector, Heat - Thermostatic type switch designed for installation on metal doors. The heat from a cutting torch will open the switch and causes an alarm to be generated.
13. Detector, Motion - A device which detects the movement of an object within an area and causes an alarm to be generated.
14. Detector, Photo-electric - Detection device which utilizes a beam of light projected into a photocell to detect an intruder. A person walking through a light beam blocks the light from the photocell which causes an alarm to be generated.
15. Detector, Vibration - A device which detects vibration caused by an attempt at forceful entry through walls and/or ceilings and causes an alarm to be generated.
16. Fail Safe - Feature which automatically activates an alarm in the event component part of the system is removed or when a component part or portion of the circuit, including the power supply, fails to function.

17. Foil - Very thin metal strips which are cemented to a glass window or door. The foil is connected to a closed electrical circuit. If the glass is broken and breaks the foil, the circuit will be opened causing an alarm.
18. Line, Alarm - An electrically supervised pair of wires connected between the detection equipment in the protected area and the monitor equipment for the purpose of transmitting alarm indications.
19. Panel, Monitor - An indicating device which provides audible and visual indications of alarm conditions.
20. Protection, Area - Protection of the inner space or volume of a secure area rather than the perimeter of the area.
21. Protection, Interior Perimeter - A system which protects the walls, doors, windows, vents and sometimes the floors and ceilings of the area.
22. Protection, Point - A system for protecting a specific object such as a safe or filing cabinet by the use of a capacitance detector.
23. Supervision, Line - Electrical protection of an alarm line. This is accomplished by having a continuous signal through the circuit. A change in signal will be detected by a monitor. The monitor gives an alarm if the change in signal exceeds the allowable tolerance for the designated type of line supervision being used.
24. Switch, Balanced Magnetic - A balanced magnetic switch operates on a balanced magnetic field in such a manner as to prevent compromise by the application of an external magnet. The system is usually mounted on a door with the switch on the door frame, the magnet on the door proper. Opening the door causes an alarm to be given.

25. Switch, Day/Night - Same as access/secure control.
26. Switch, Door - A switch usually magnetically operated, which opens its contacts when the door which is being protected opens. The switch is usually mounted on the door frame and the magnet which operates it is usually mounted on the door. The switch is connected in series with a closed alarm circuit. Opening the circuit causes an alarm to be generated.
27. Switch, Gate - This switch operates in the same manner as a door switch. It is enclosed in a weatherproof housing to permit outdoor use.
28. Switch, Tamper - A switch in the security equipment enclosure which opens the alarm line circuit if the enclosure is opened causing an alarm.

TYPICAL LOCAL ALARM SYSTEM

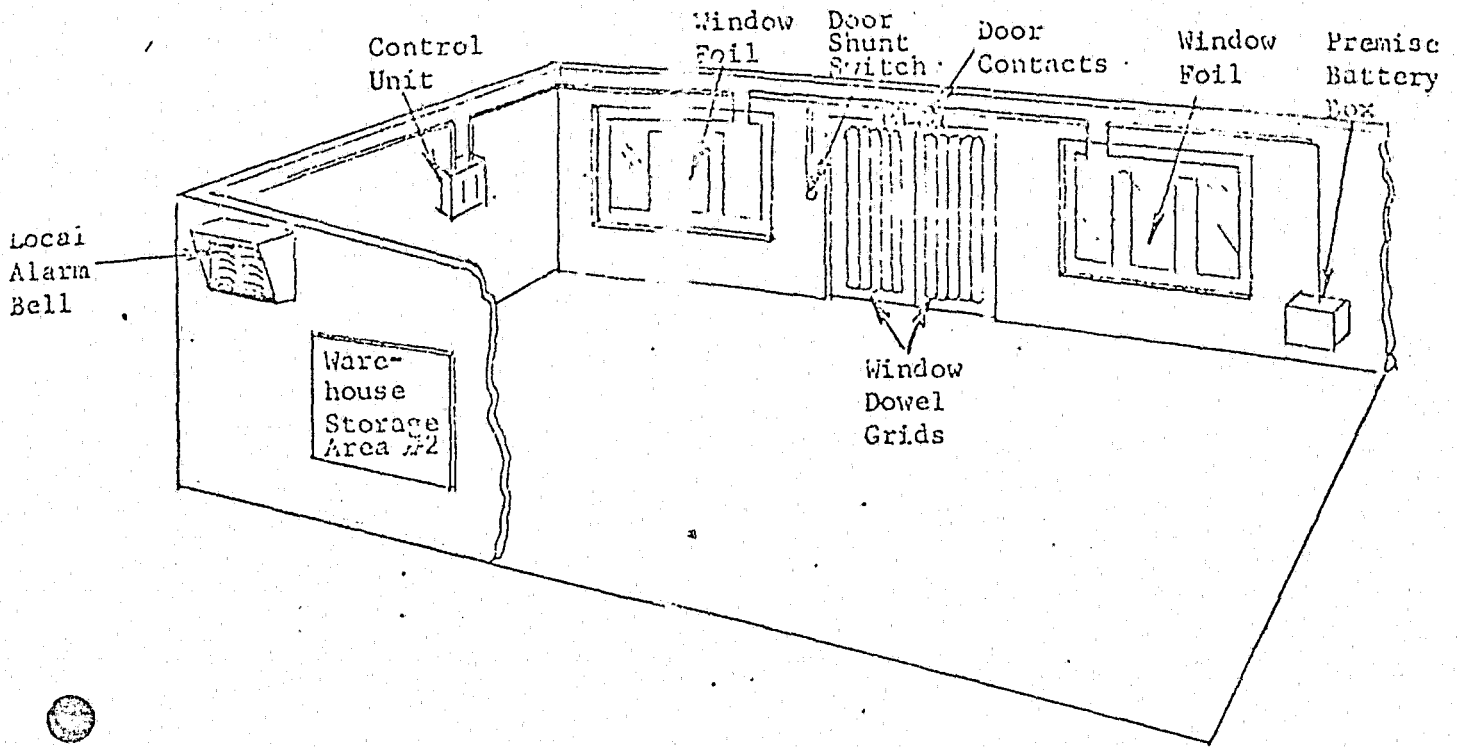


FIGURE 1

SECTION II

TYPES OF SYSTEMS

A. General

Intrusion detection systems are divided into three general categories. The classification of an intrusion detection system into one of the three categories is determined by the method in which the alarm signal is annunciated and the location of this alarm signal. The three categories are as follows:

1. Local Alarm System - A local alarm system is one in which the alarm device such as a bell, horn, claxton, etc., is located in the immediate vicinity of the protected area or object. A typical application of this type of alarm would be in a storage facility with a bell mounted on the outside of the protected area or externally mounted to the outside of the building proper, to sound an alarm (See Figure 1).

The effectiveness of this system relies on the psychological effect of the noise of the alarm and the chance or programmed response of nearby military police or military personnel. This system may be used in conjunction with a proprietary alarm system as described below.

2. Proprietary Alarm System - A proprietary alarm system is one in which the alarm signal is relayed to a location which is manned and operated at a guard office. An example of this type of system would be one consisting of many buildings containing alarm systems, which are monitored at the base Provost Marshal's office or at another designated location. This type of system provides fast response to alarms by trained personnel who are equipped to handle emergency situations of this type. With the alarm sounding at a point

remote to the protected area, the intruder has no indication that he has initiated an alarm until the guards arrive on the scene to investigate. (See Figures 2 and 3).

3. Central Station Alarm System - A central station alarm system is one in which the alarm signal is transmitted to a monitor facility located at a remote point and operated by a commercial concern. When an alarm is received, the concern monitoring the system, either calls the military police, local police, or may dispatch predesignated guards to respond to the alarm (See Figure 4).

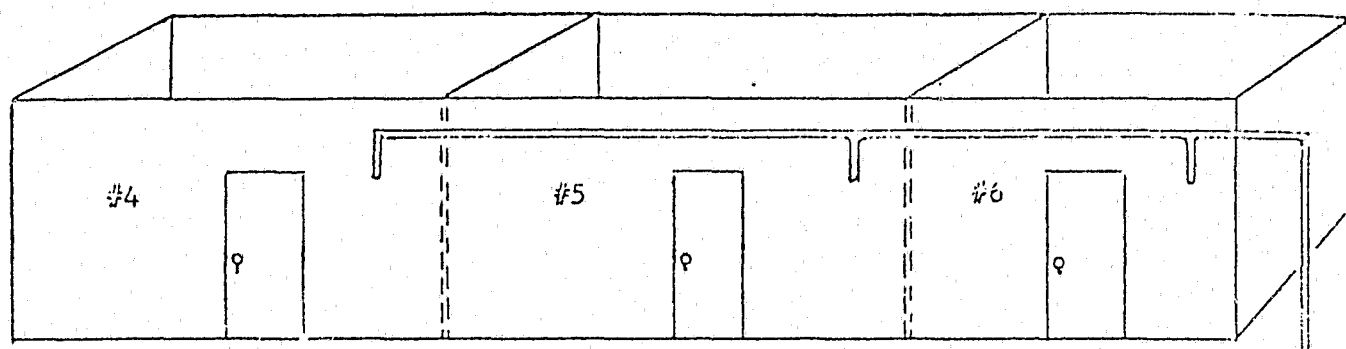
B. Functional Description of Intrusion Detection Equipment

1. General - The effectiveness of any intrusion detection system used depends upon the quality and reliability of the detection equipment, its ability to resist compromise, and the reliability and sophistication of the line supervision and monitoring facility. Minimums for construction performance of detectors, monitors and associated hardware are established in Section VI (Specifications). The following paragraphs define those detectors and monitors and outline their general application and reliability.

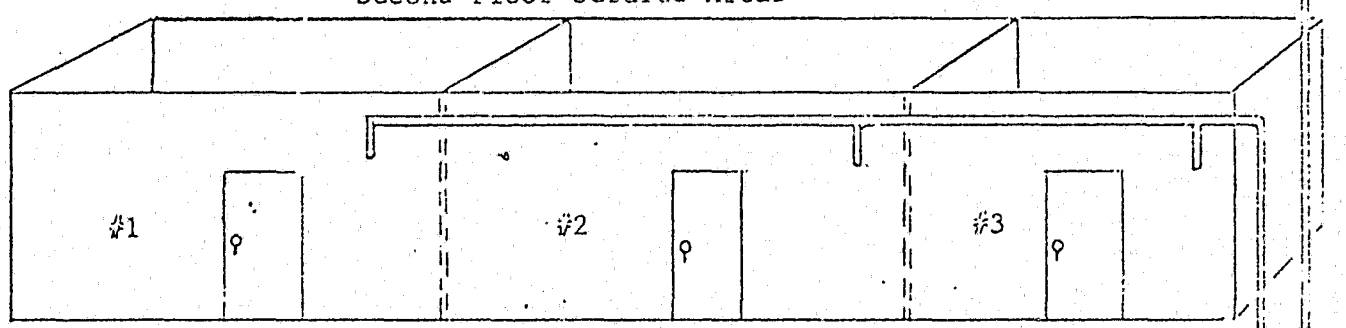
2. Electro-Mechanical Devices - The detection devices in this category are simple and balanced magnetic switches, window and wall foil, protective wire, hold-up buttons and foot rails and heat detection devices. All of these detection devices function through an access/secure control unit. The description of and general application of these devices is as follows:

a. Access/Secure Control Unit - This unit serves as the termination device for electro-mechanical detectors. (See Figure 5) It furnishes power to the detector when required, transmits the "Alarm Condition" to the monitor panel, furnishes

TYPICAL PROPRIETARY ALARM SYSTEM INSTALLED



Second Floor Secured Areas



First Floor Secured Areas

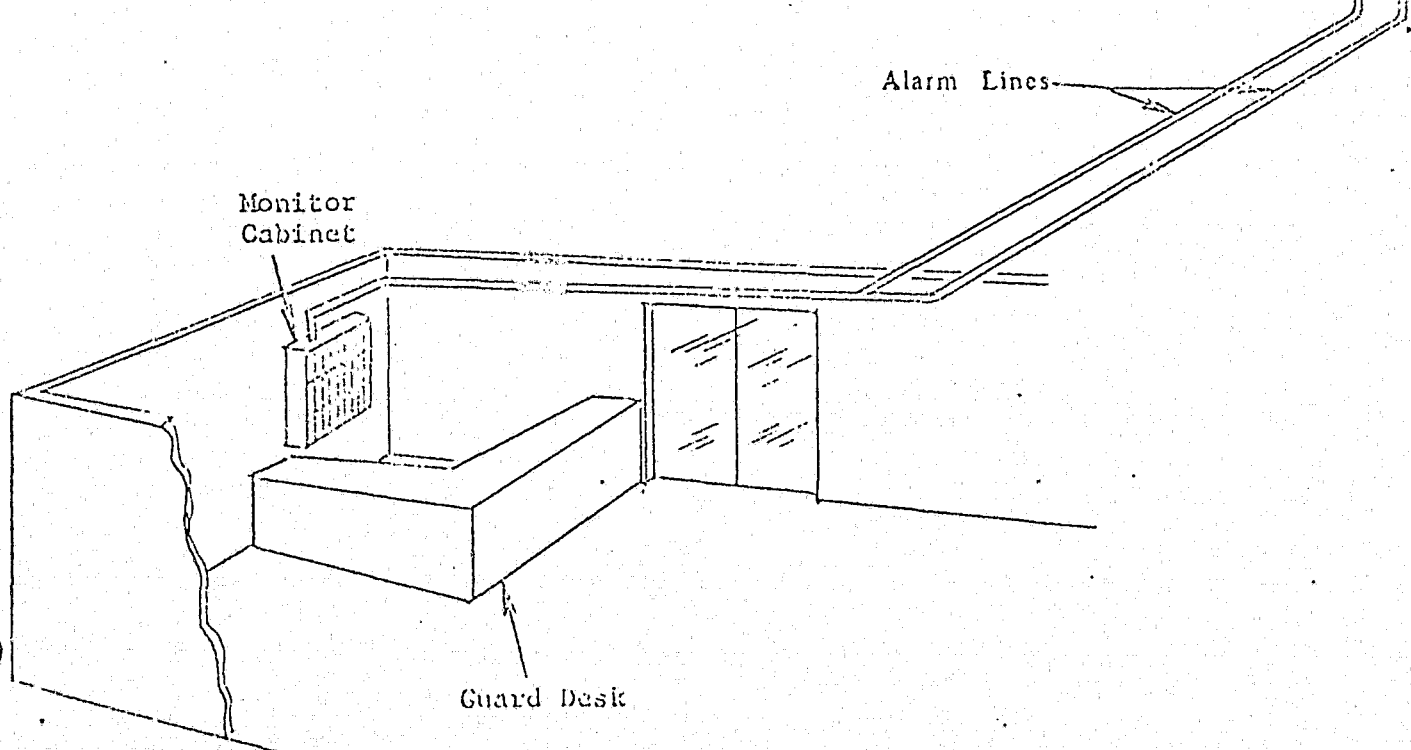


FIGURE 12

TYPICAL PROPRIETARY ALARM SYSTEM INSTALLED ON A MILITARY BASE

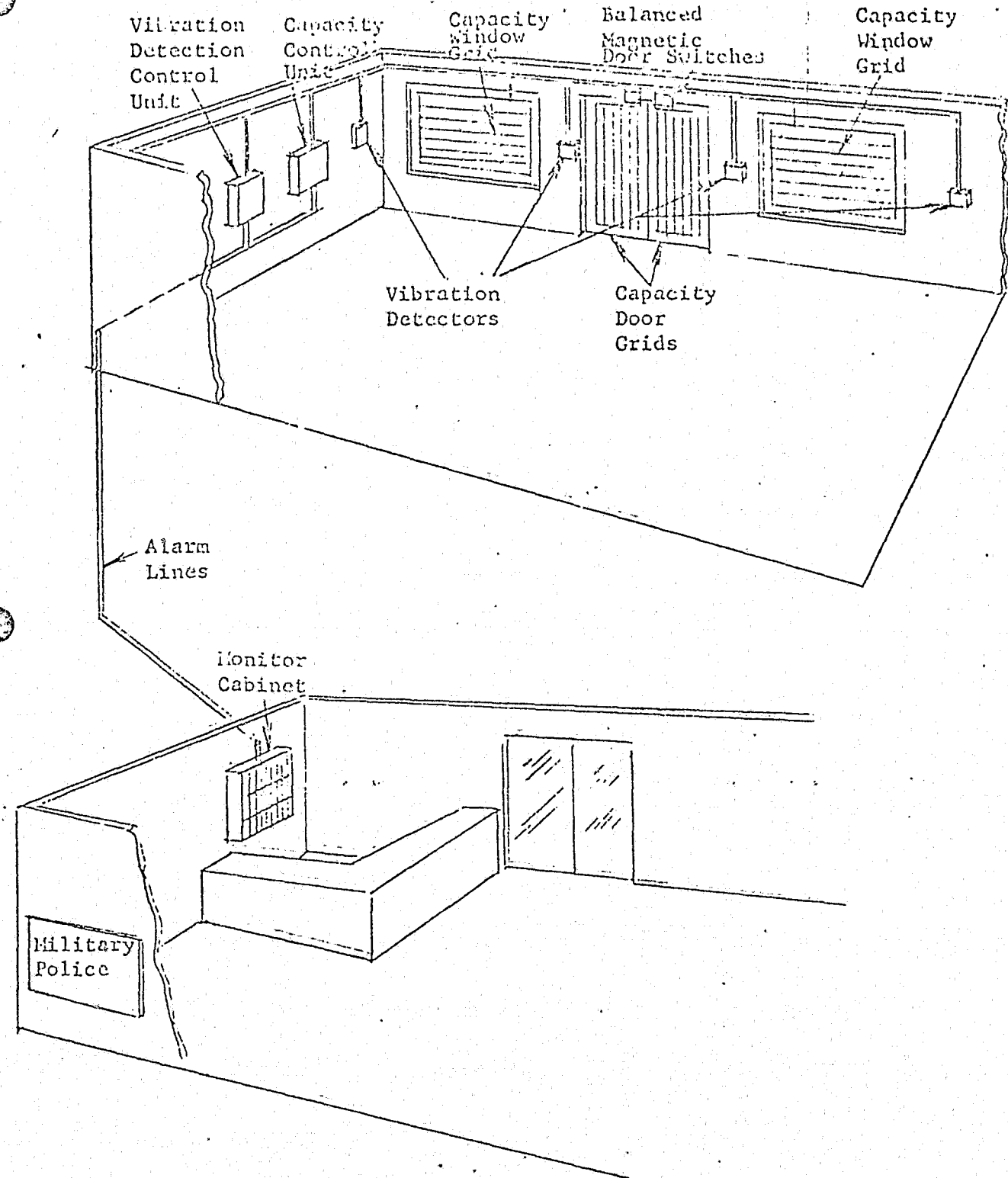


FIGURE 3

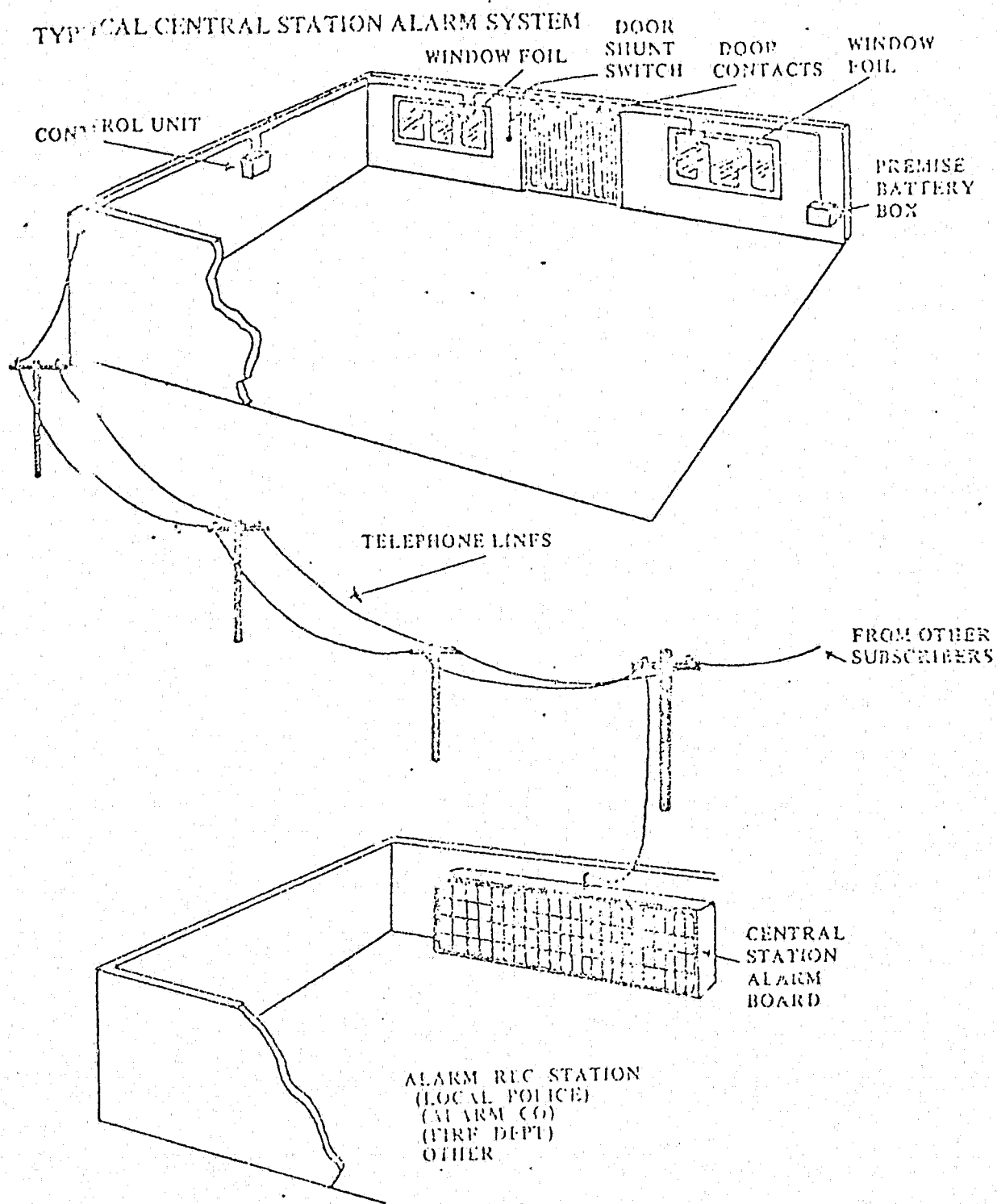
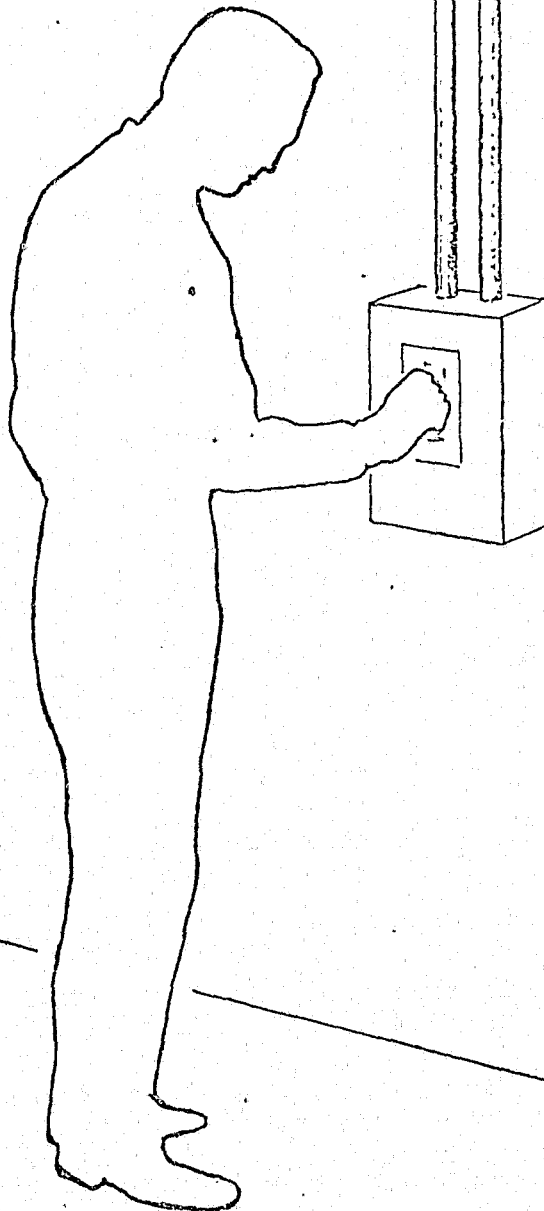


FIGURE 4

TO MONITOR PANEL.



ACCESS/SECURE CONTROL UNIT

(Located inside the Secure Area)

FIGURE 5

termination circuitry for "Line Supervision" of the alarm transmission line, furnishes circuitry for tamper devices within the detection devices and indicates whether the protected area is in the access or secure mode. Each zone of electro-mechanical protection should have an access/secure control switch. This device should be located within the secured area proper.

b. Magnetic Switches

(1) Simple Switch - A simple magnetic switch consisting of a switch housing and a magnet housing. A switch housing contains the wiring and a magnet actuated reed switch. The use of the simple magnetic switch is normally associated with intrusion detection systems protecting movable openings in facilities containing low dollar value items since this type switch can be easily defeated.

(2) Balanced Switch - A balanced magnetic switch consists of a switch housing and a magnet housing. The switch is enclosed in a cast nonferrous housing which provides a hub type or threaded outlet so that the system may be run in conduit if desired. The housing contains a tamper switch to detect unauthorized opening of the switch housing. The switch itself is designed so that it cannot be defeated by the increase or decrease in the magnetic field caused by the introduction or removal of a magnet from the proximity of the switch.

Balanced magnetic switches are used to protect movable openings in facilities containing high dollar value items, sensitive items or classified information, i.e., classified information storage vaults, bank vaults, sensitive operations areas, conference rooms and arms storage areas. (See Figure 6.)

c. Foil - Foil systems function as a part of a completed circuit that, when broken, causes an alarm. (See Figure 7) Foil systems normally consist of metallic tape applied to glass surfaces or mounted on masonite or plywood panels used in walls, floors and ceilings.

Foil is used in facilities containing low dollar value items, since the system can be readily defeated.

d. Protective Wire - Protective wire functions as a part of a completed circuit that, when broken, causes an alarm. (See Figure 8) Protective wire systems come in many forms; wire traps, single wires insulated and strung over irregularly shaped openings; screens or single wires cemented into wooden dowels and frames adapted to cover various sized openings, and lacing or wire attached to masonite or plywood panels used to supplement wall construction. This system, like foil, is normally used to protect openings in the perimeter or low priority area since the system can be readily defeated.

e. Hold-up Devices - Holdup alarms are mechanical switches which are used to open an alarm circuit when actuated by a person. (See Figure 9) This device comes in many forms most popular of which are holdup buttons and foot rails.

(1) Holdup Buttons - Holdup buttons are mechanical switches specially constructed to avoid accidental actuation. Some of these switches require actuating two levers or buttons at the same time and some have metal ridges which protect a single button and require that the button be pressed at least 3/8" below the protective ridge. This device is used in all priority areas where there is public contact, i.e., bank officers desks, isolated or very sensitive guard posts, VIP suites, etc.

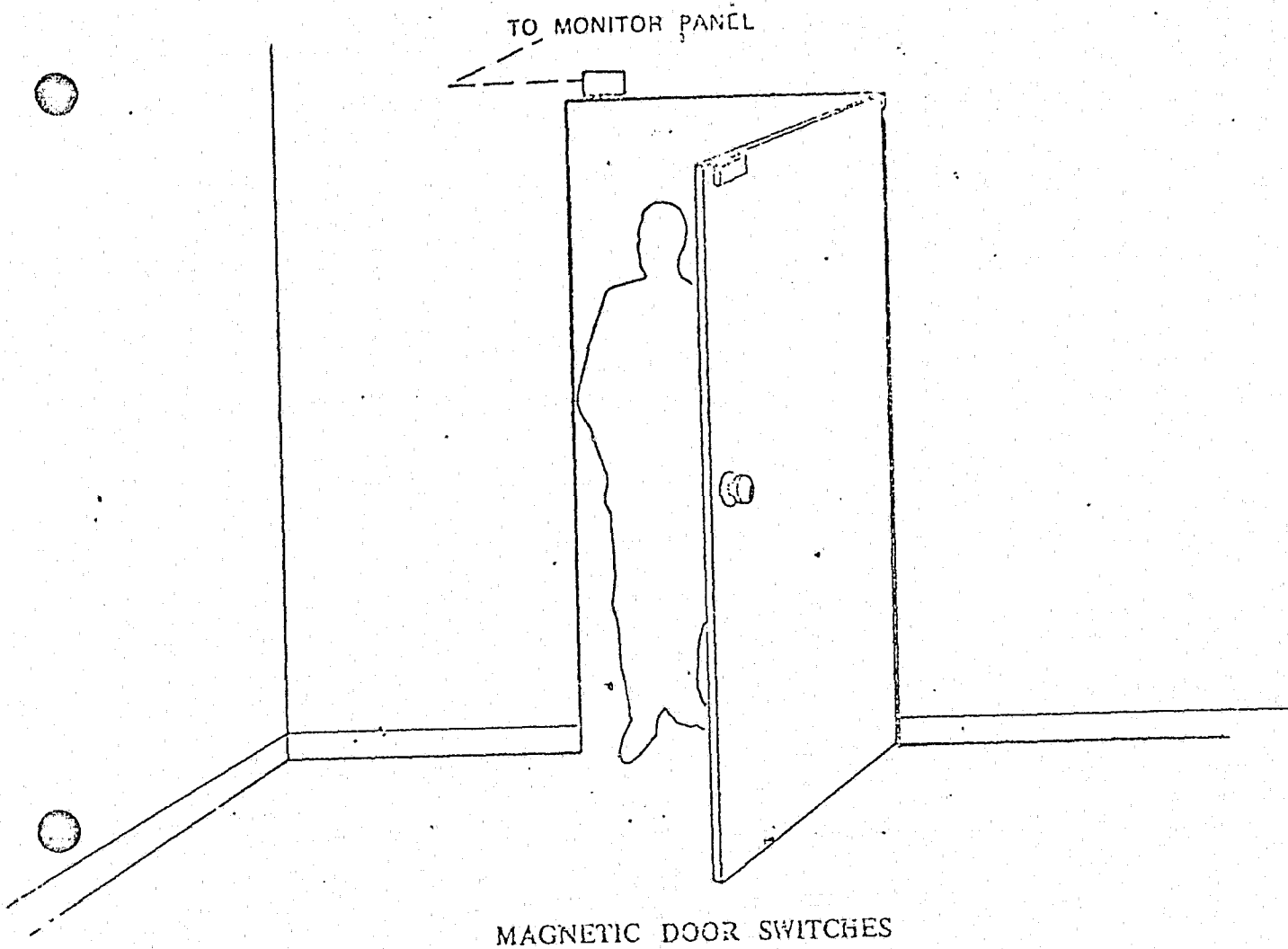
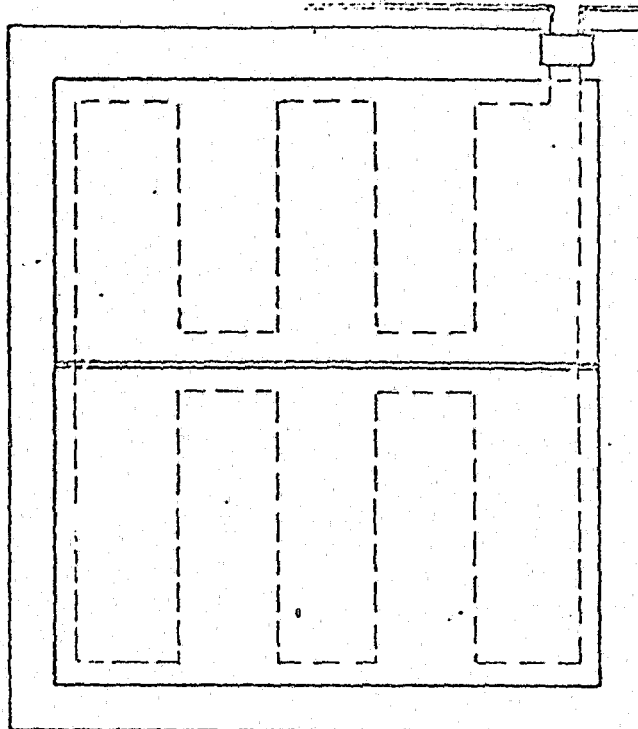


FIGURE 6



WINDOW FOIL

FIGURE 7

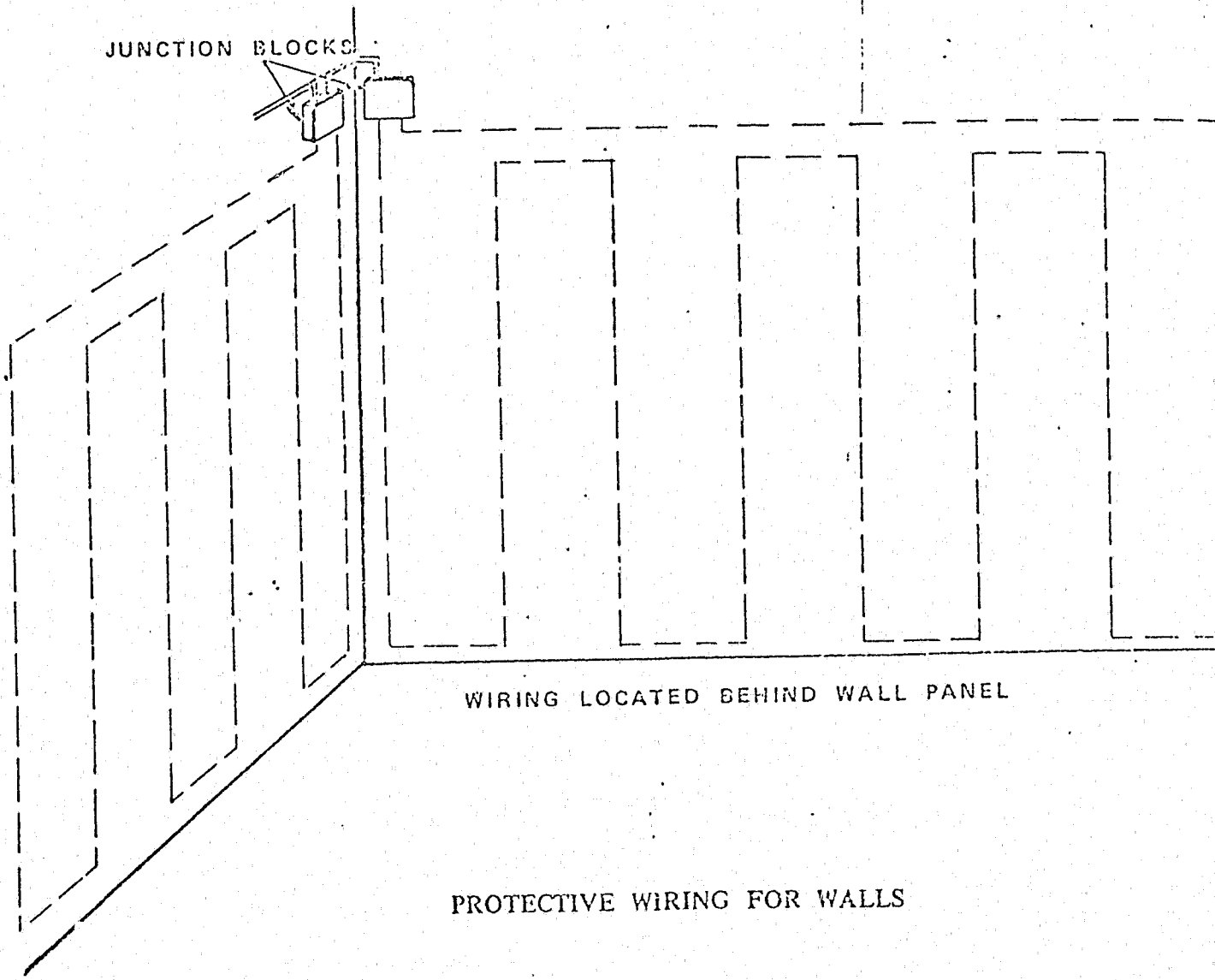
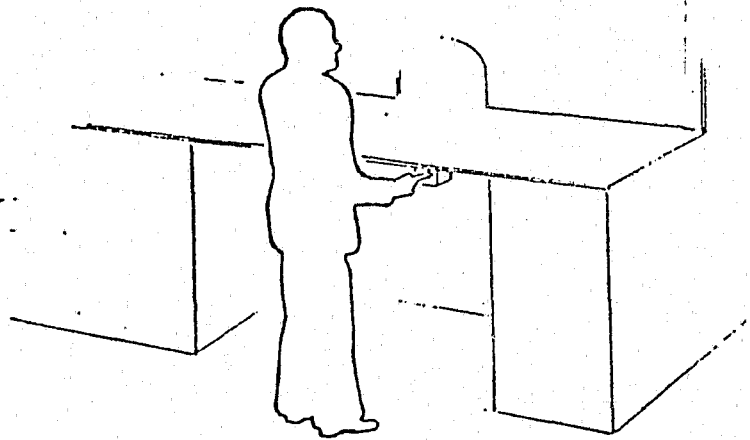
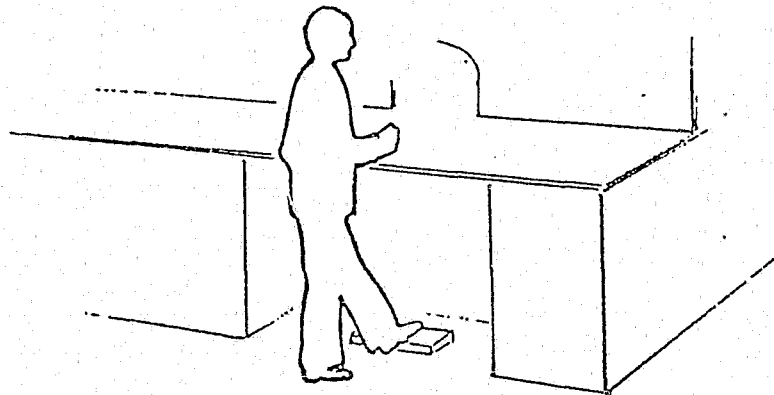


FIGURE 8



PUSH BUTTON

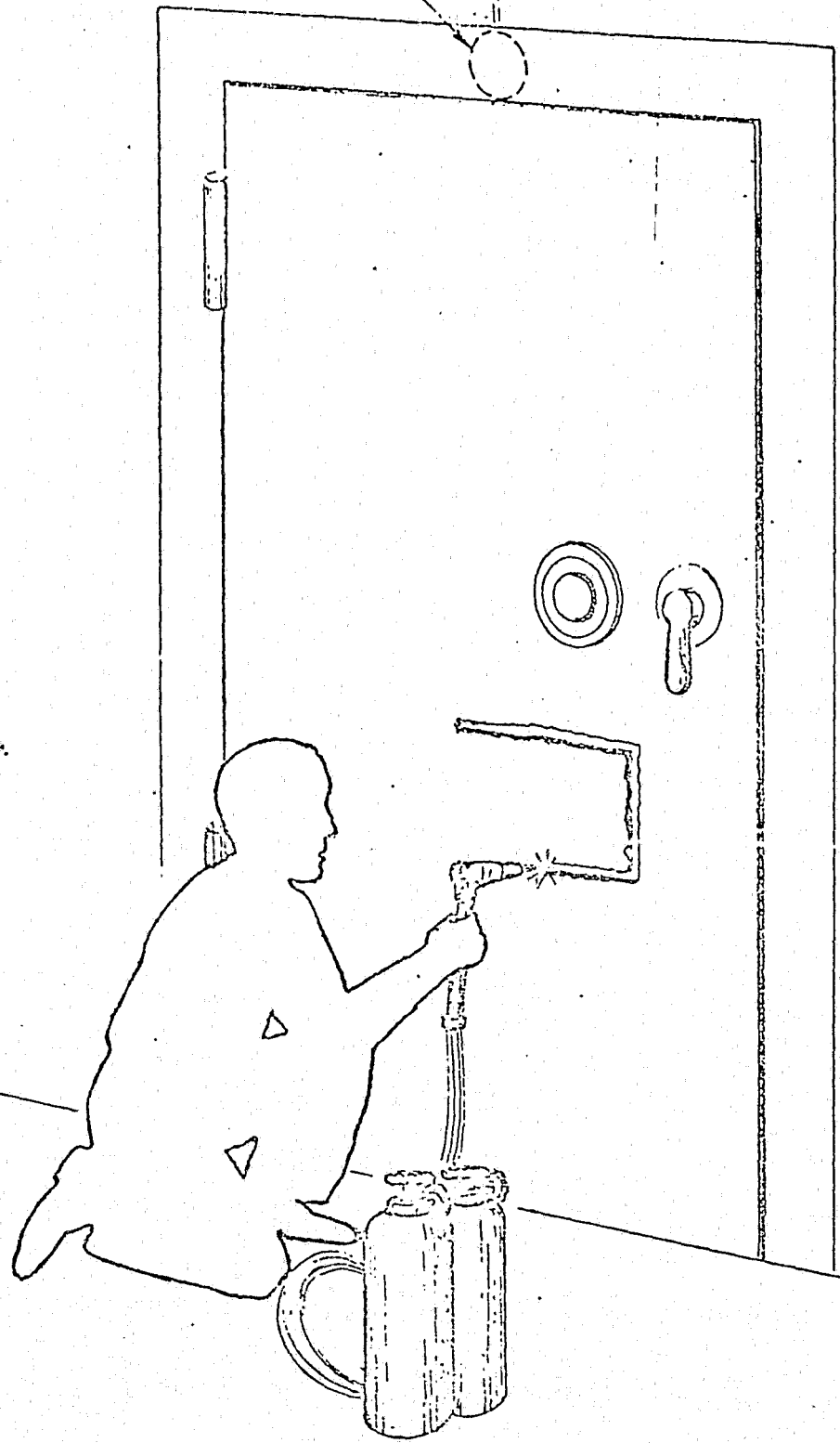


FOOT RAIL

HOLDUP DEVICE

HEAT DETECTOR

TO MONITOR PANEL



HEAT DETECTOR

FIGURE 10

(2) Hold-up foot Rails - Foot rails are mechanical switches specially constructed to be actuated by the foot and at the same time avoid accidental actuation. Most floor rails require a subtle but purposeful movement of the foot requiring the user to reach under the rail and press upward with the toe.

Most buttons and foot rails are also equipped with "Key Reset" devices which require that a key be used to reset the switch after it has been actuated. Normally, the key is in the custody of the response force.

Foot rails are used at cashier's station in banks, finance offices and exchanges, isolated or sensitive guard post, etc.

f. Heat detectors - Heat detectors are mechanical switches actuated by the presence of heat. (See Figure 10) The switches or thermostats are housed in a protective metal shell or dome. The heat detectors consist of a rate of rise section (which actuates when the temperature rise exceeds 5 degrees in 20 seconds) and a fixed temperature section (which actuates when temperature exceeds a present level such as 135° or 185°).

Heat detectors are used at places in the perimeter or on object protection where burning may be anticipated as part of an attempted entry or theft.

3. Photo-Electric Devices - Photo-Electric devices consist of a two part system, a light source or transmitter and a receiver. (See Figure 11). This system functions when the light beam between the transmitter and receiver is totally or partially broken. The light transmitter uses a modulated infrared

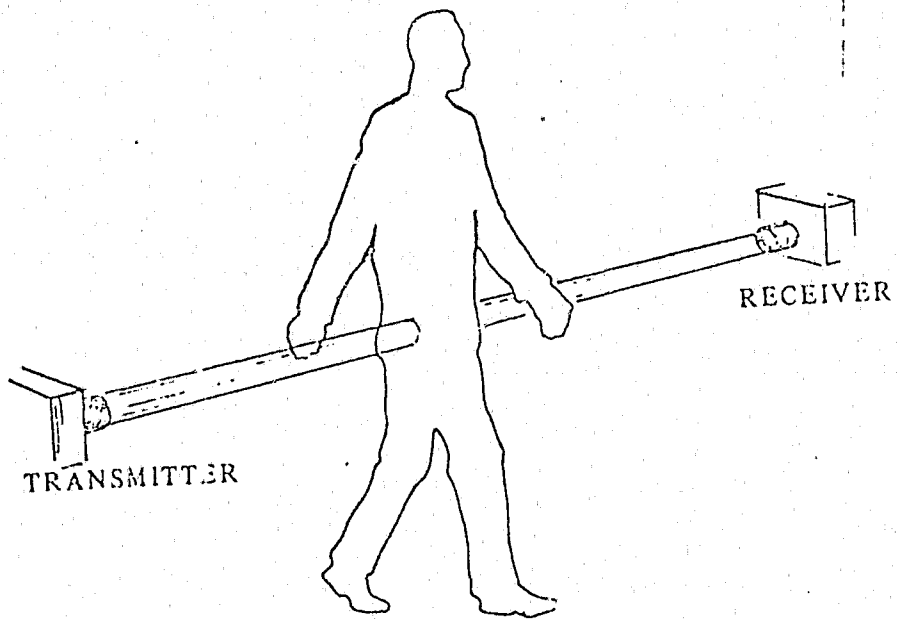


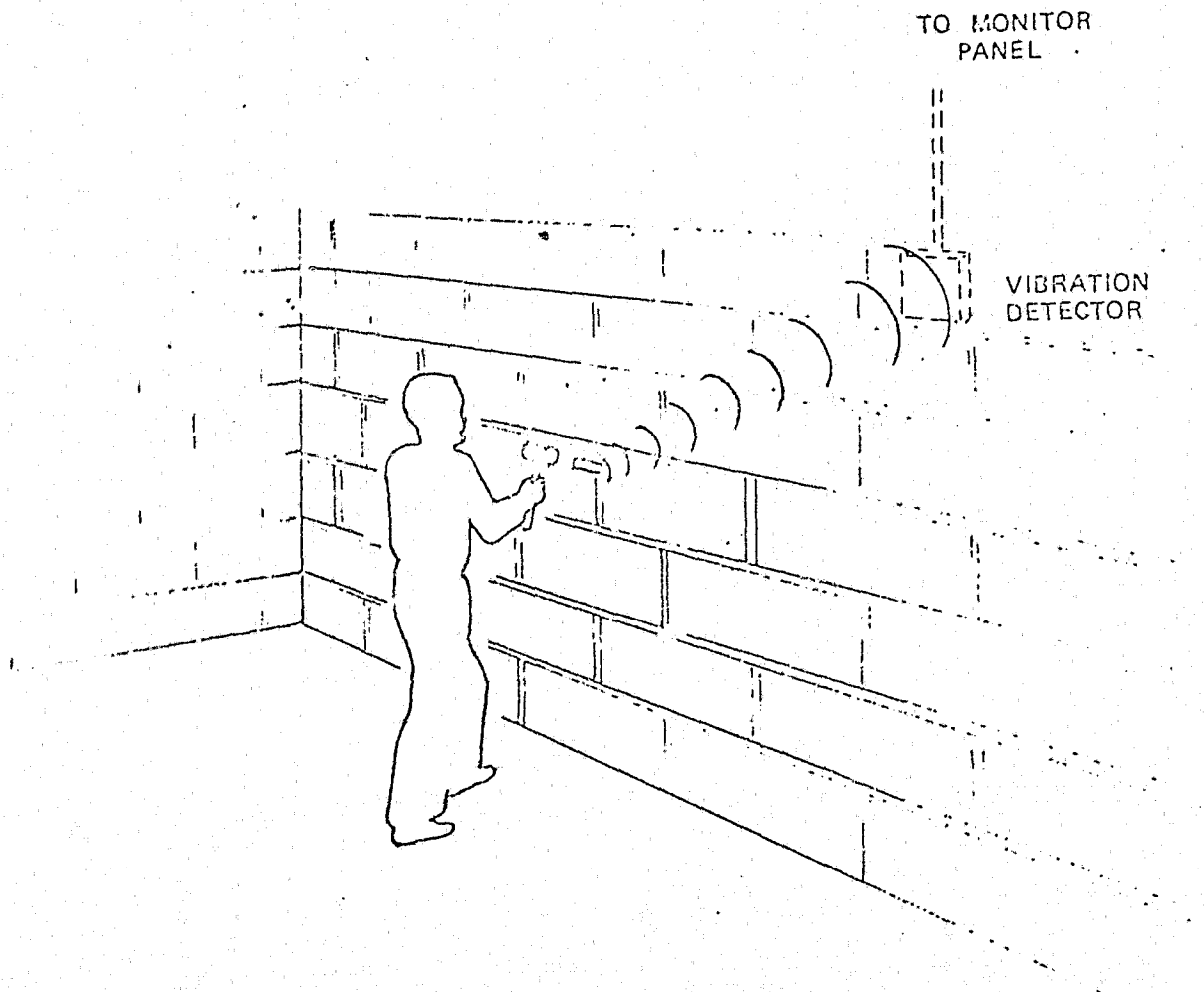
PHOTO ELECTRIC SYSTEM

light beam which is used instead of visible light to prevent false alarms in the system. Light may be transmitted directly from transmitter to receiver or it may be bent by mirrors to achieve better coverage.

This system is used as a part of the perimeter protection for low priority areas such as warehouses and storage areas.

4. Vibration Detection Systems - Vibration detection systems consist of a control unit containing an amplifier, an accumulator and a power supply. (See Figure 12) The amplifier accepts a signal from a group of vibration pickup devices which may be mounted on walls, doors or ceilings of a protected perimeter, and drives the accumulator circuits to a point where it triggers an alarm. The protection system amplifier has an adjustable gain so that the number of impulses required to cause an alarm is adjustable. The accumulator circuitry has the ability to bleed back to zero if the required number of impulses is not received over approximately a 20-minute period. The vibration detection systems are used to detect attempted forceful entry through walls, and ceilings of the protected area, and are normally installed in high priority perimeter protective systems, i.e., arms storage rooms, bank vaults, sensitive security and operations areas.

5. Audio Detection Systems - Audio detection systems consist of a control unit containing an amplifier, an accumulator and a power supply. (See Figure 13) The amplifier accepts a signal from a group of audio pickup devices which are mounted on the walls of a protected area. The protection system amplifier has an adjustable gain so that the number of sounds required to cause an



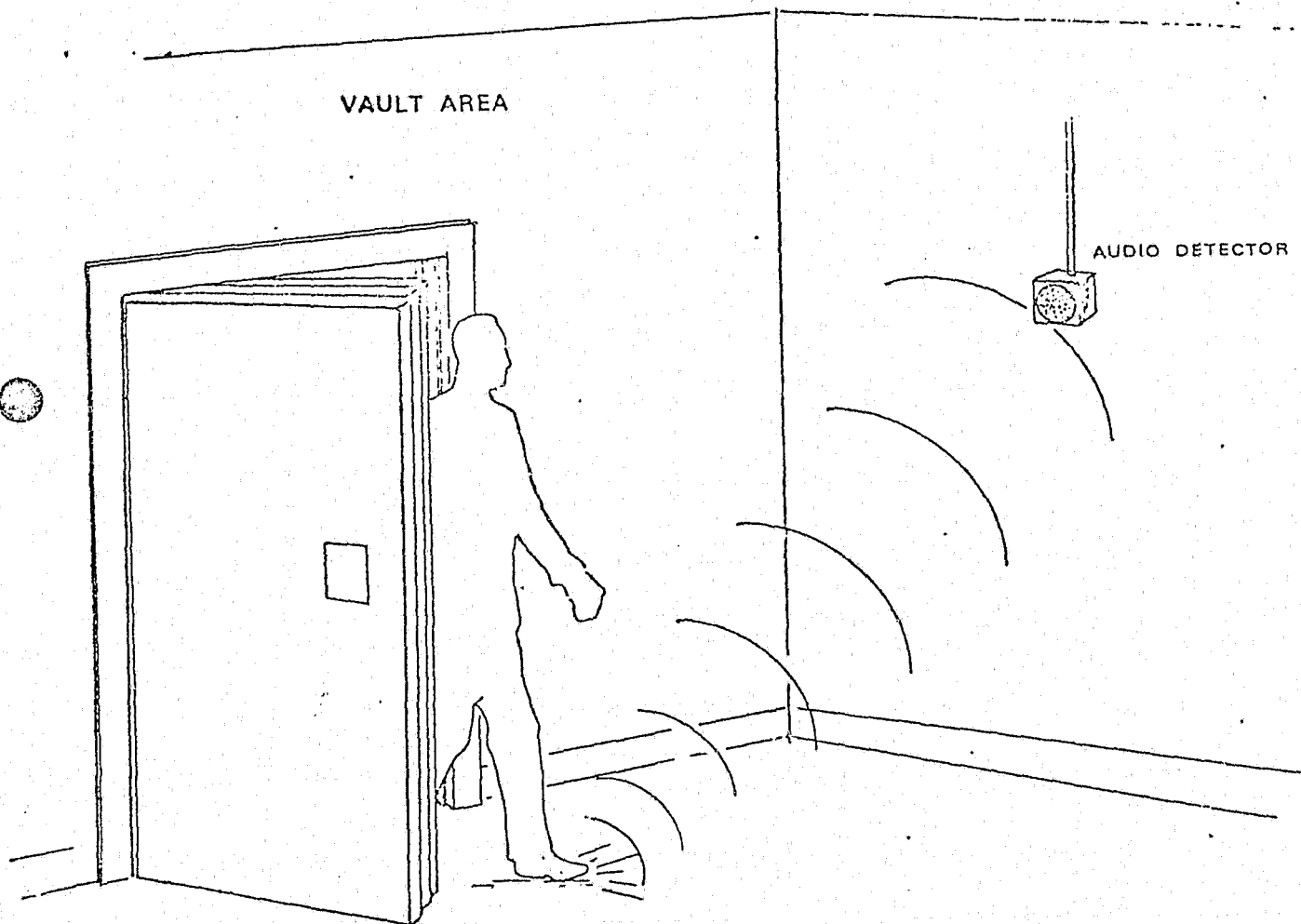
TO MONITOR
PANEL

VIBRATION
DETECTOR

VIBRATION DETECTOR SYSTEM

VAULT AREA

AUDIO DETECTOR



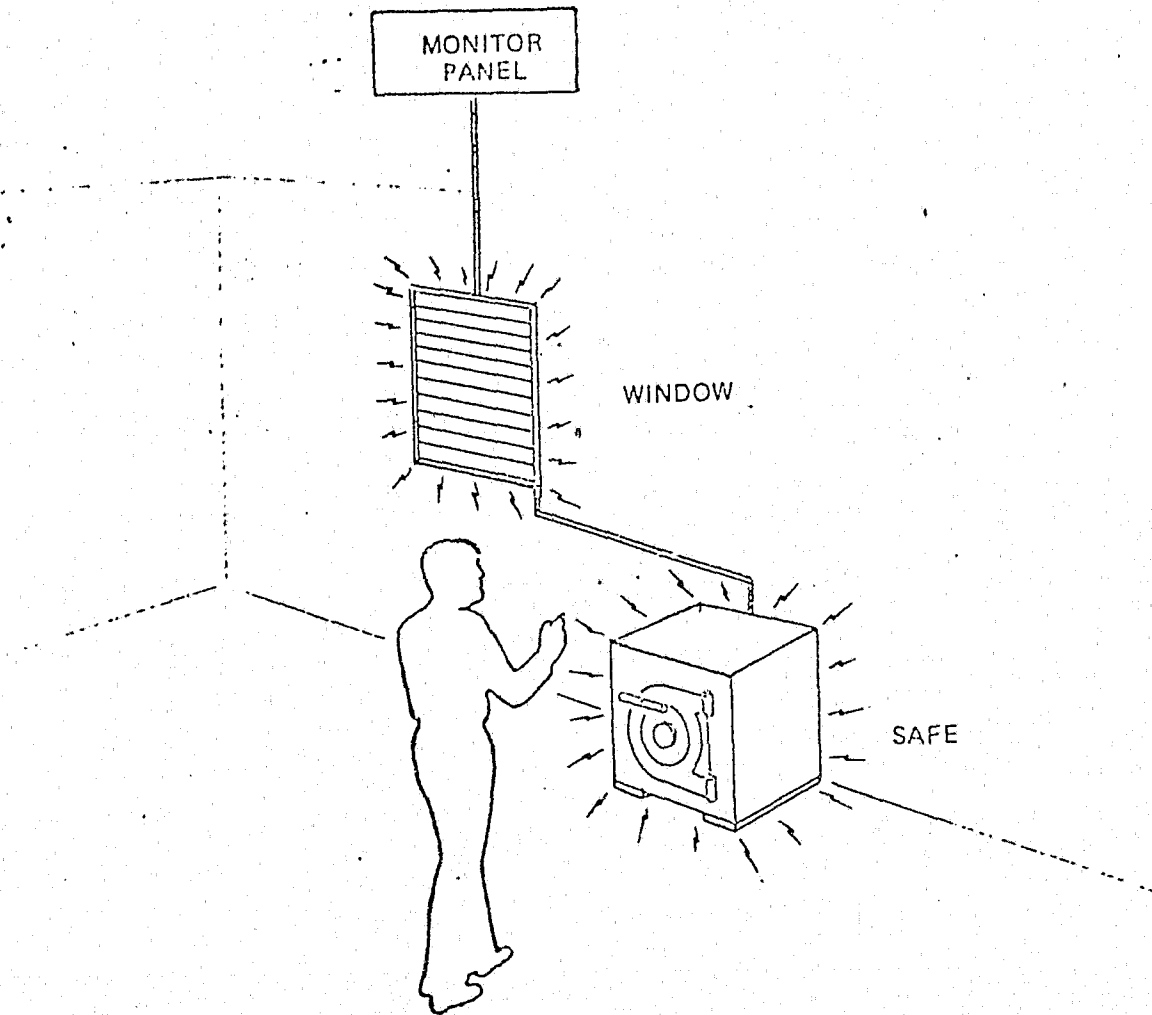
AUDIO DETECTION SYSTEM

FIGURE 13

alarm is adjustable. The accumulator circuitry has the ability to bleed back to zero if the required number of impulses is not received over approximately a 20-minute period. The audio detection system is used to detect sounds generated by attempted forceful entry through walls, and ceilings of the protected area, and are normally installed in high priority perimeter protective systems, i.e., arms storage vaults and bank vaults. The audio detection system is to be used only in areas which are completely sound proofed.

6. Capacitance Detection Systems - Capacitance alarm systems consist of a control unit which will detect the approach or contact of an object coming in proximity to the capacitance grid or a container which is forming a part of the tuned circuit of the equipment. (See figure 14) This equipment is sensitive to the increase or the decrease in capacitance when an object is introduced into the field or removed from the field of protection. When this occurs, an alarm will result. Capacitance grid systems are used to protect ceilings, window openings, substandard doors, air conditioning and heating ducts in the perimeter of the protected area, for object protection on containers or safes used for storage of valuable merchandise or classified information. These applications are for both high and low priority areas, i.e., sensitive security operations areas and vaults, arms storage areas, bank vaults, post exchange money chests, etc.

7. Motion Detection Systems - Motion detection systems operate on the basis of detecting "doppler effect" by using a device which transmits a given frequency within a closed area to a receiver also located in the closed area.



CAPACITANCE DETECTION SYSTEM

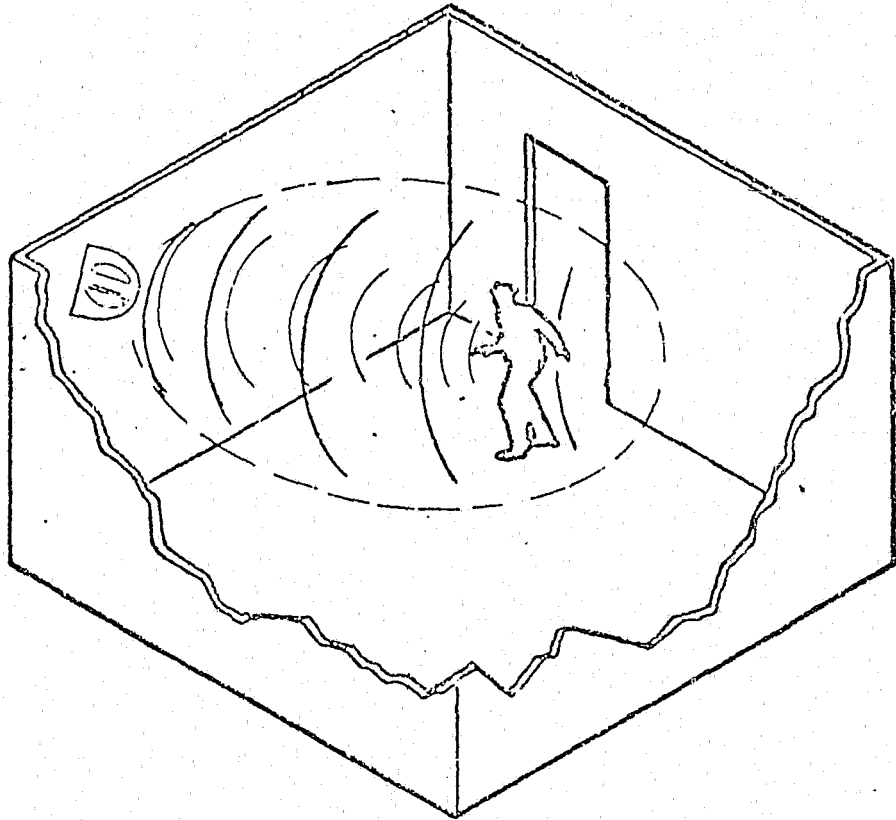
FIGURE 14

A control unit detects any frequency shift "doppler effect" caused by a moving body within the field of surveillance. (See Figure 15). There are three basic types of motion detection, the major differences between the three are the frequency used for surveillance. The following systems are those most commonly used.

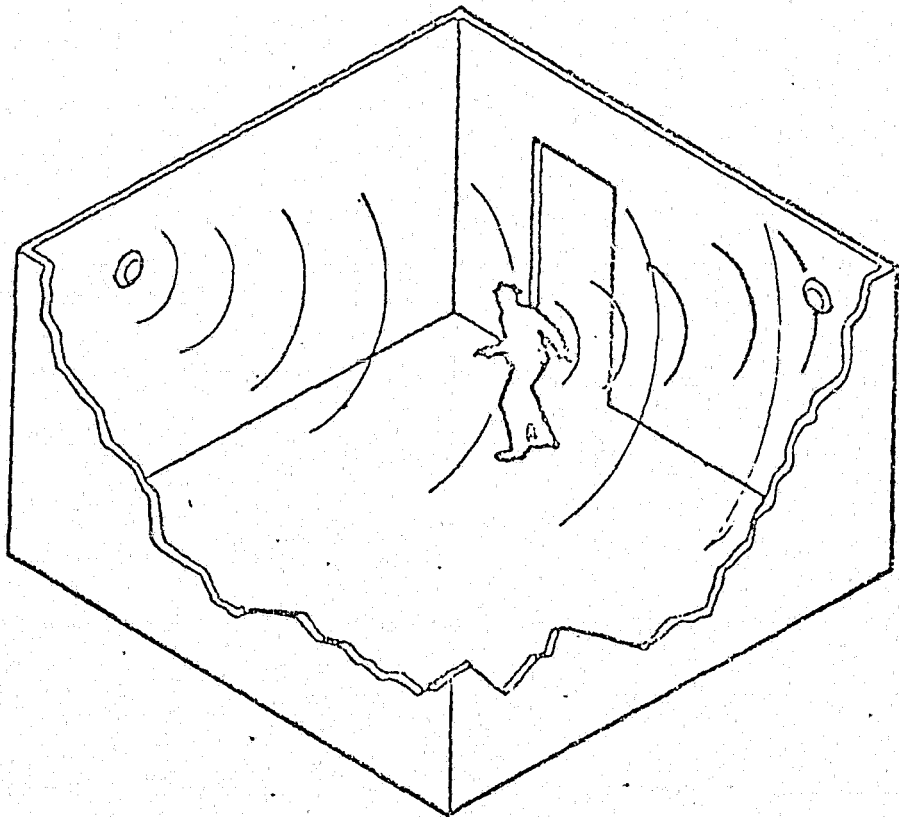
a. Sonic - The transmitter used in this system emits a continuous audible signal to form the necessary wave patterns to fill the area protected. The sonic motion detection system is used in both high and low priority area protections, i.e., warehouses, security vaults, etc. Limiting factors which must be considered before using this system are whether the audible signal will be an annoyance to personnel who may be required to work in close proximity to the system, or whether the system will conflict with perimeter protection devices such as vibration and audio detection systems.

b. Ultra-sonic - The transmitter used in this system emits a signal above the audible range of the human ear. The ultra-sonic motion detection system is used in both high and low priority area protection, i.e., post exchange store rooms, weapons storage areas, sensitive operations areas, etc. The presence of extreme air motion turbulence and/or temperature inversions should be avoided for stable system operation. Areas containing water pipes, air conditioning or heat ducts which inject vibration or cause a sudden flow of air mass should also be avoided.

MOTION DETECTORS



MICROWAVE



SONIC and ULTRA SONIC

c. Micro-Wave - The transmitter used in this system operates in the micro-wave frequency region. The micro-wave motion detection system is used in both high and low priority area protection, i.e., arms storage buildings, warehouses, sensitive operations areas and conference rooms, etc.

In this system definitive micro-wave patterns are created. Therefore, several units may be required to give total protection.

C. APPLICATION

Figures 16 through 24 provides general guidance in understanding the application of equipment to meet specific needs. These illustrations should not be considered as standards for all field applications since particular equipment needs are dependent upon the indoor and outdoor environment, structural design of the protected area, and types of items being protected.

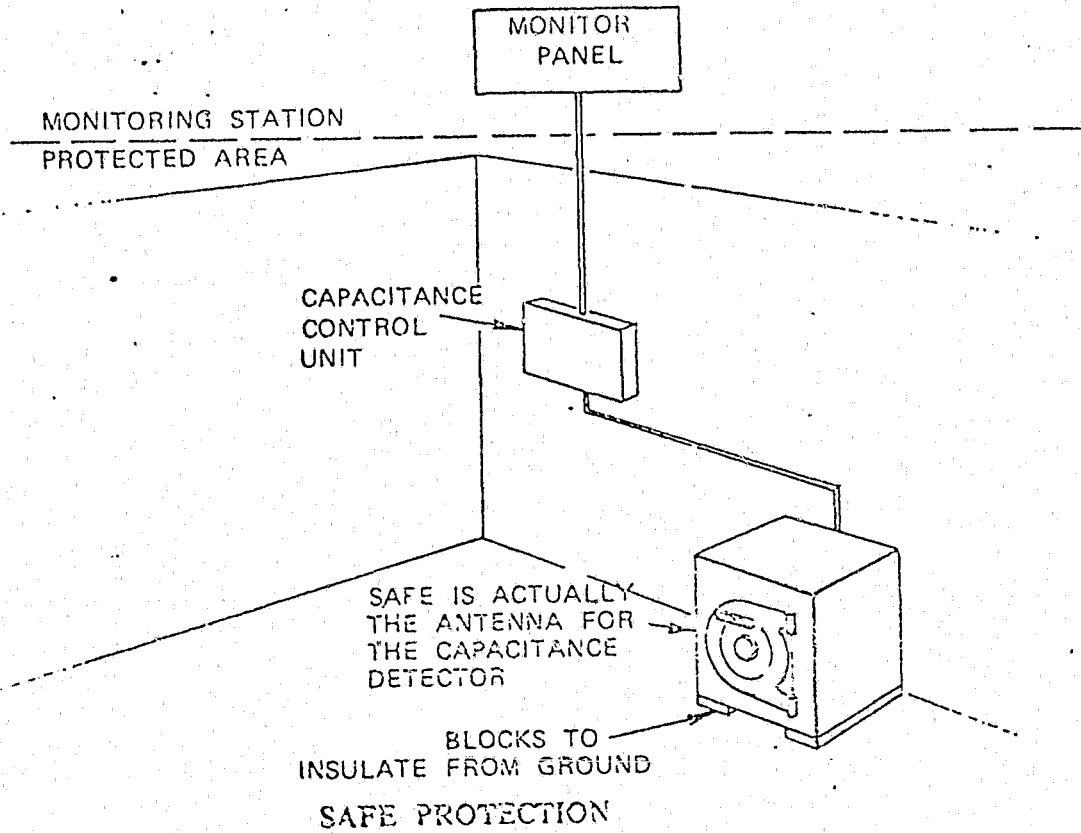


FIGURE 16

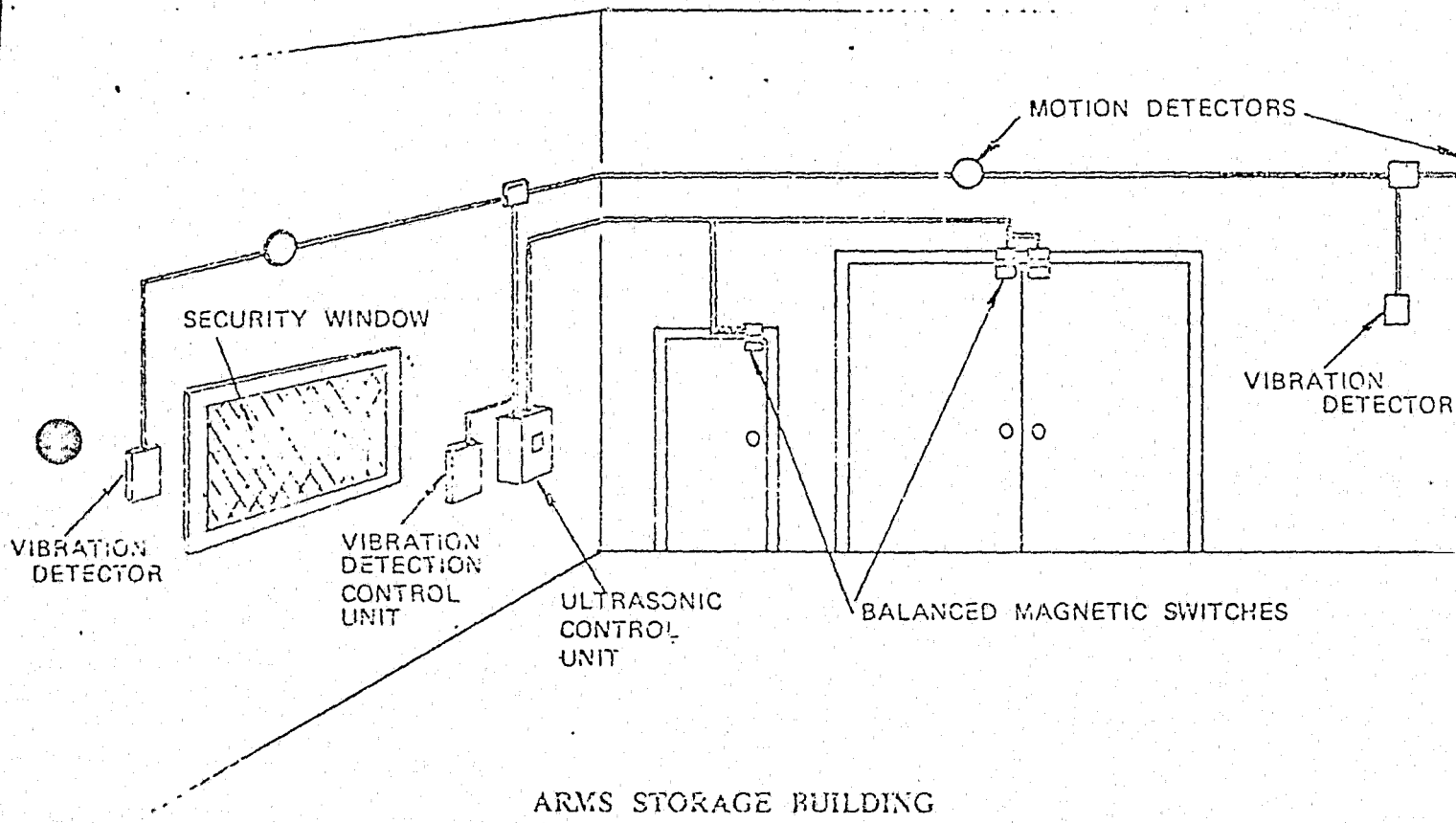


FIGURE 17

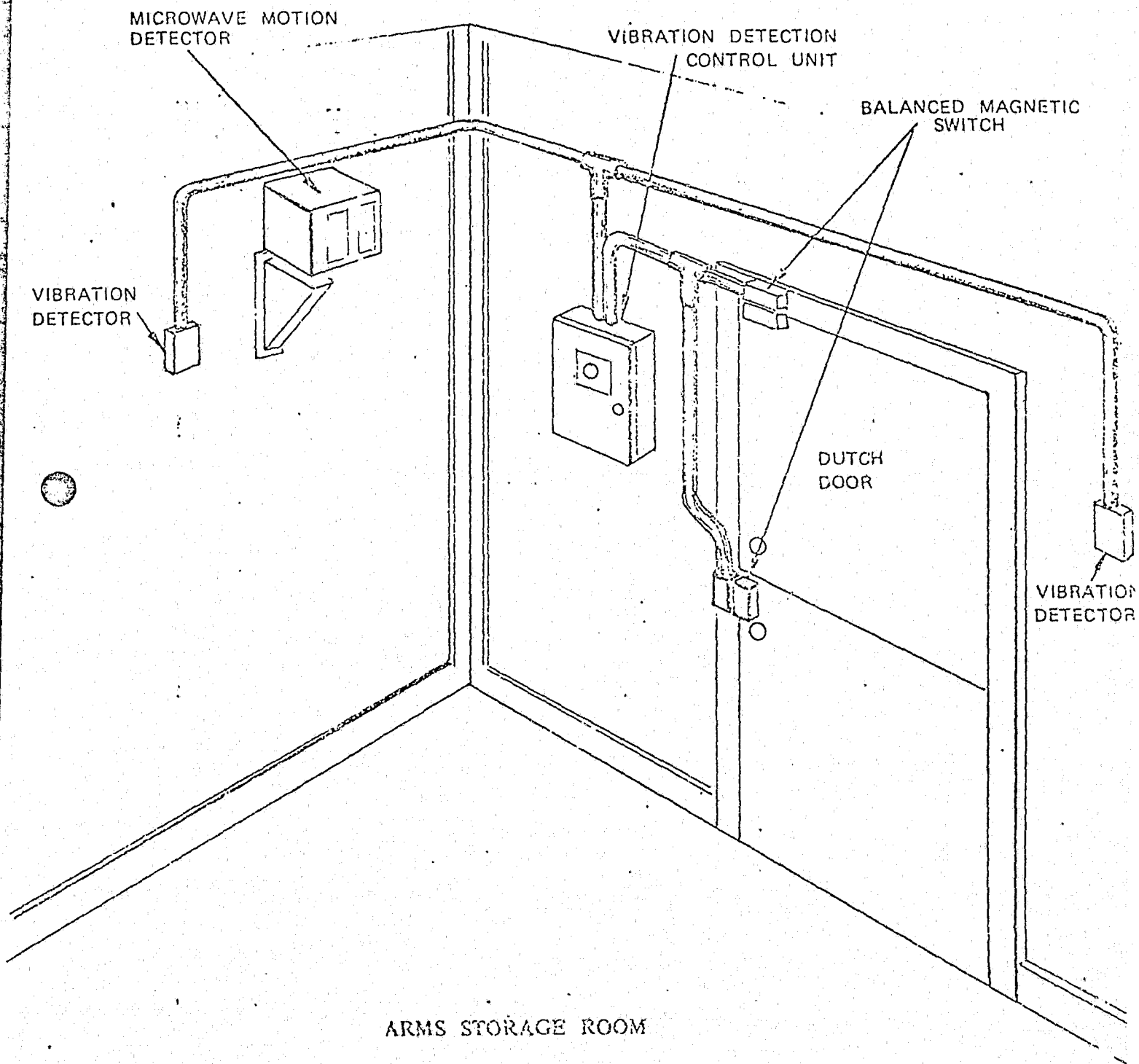


FIGURE 18

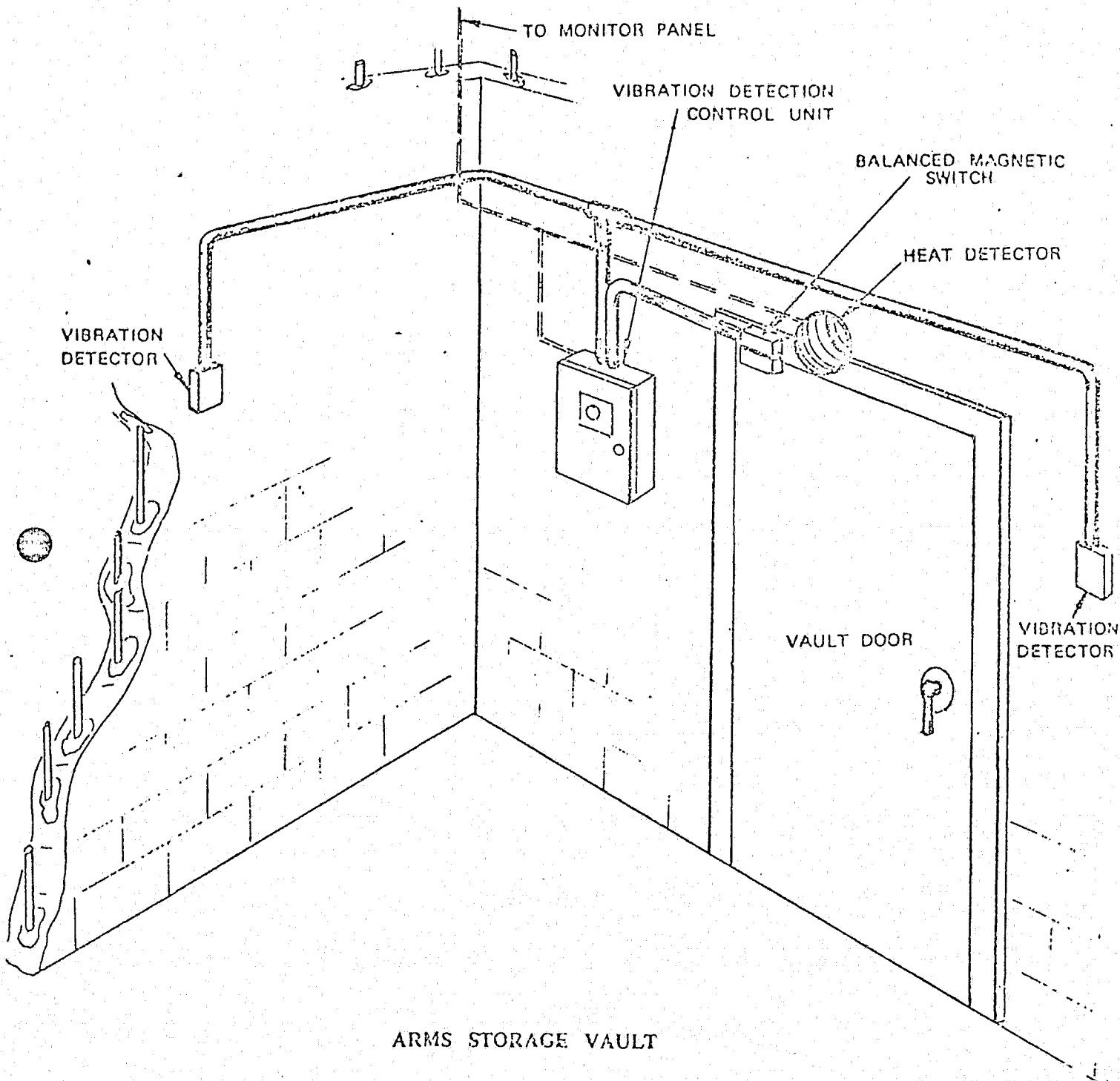


FIGURE 19

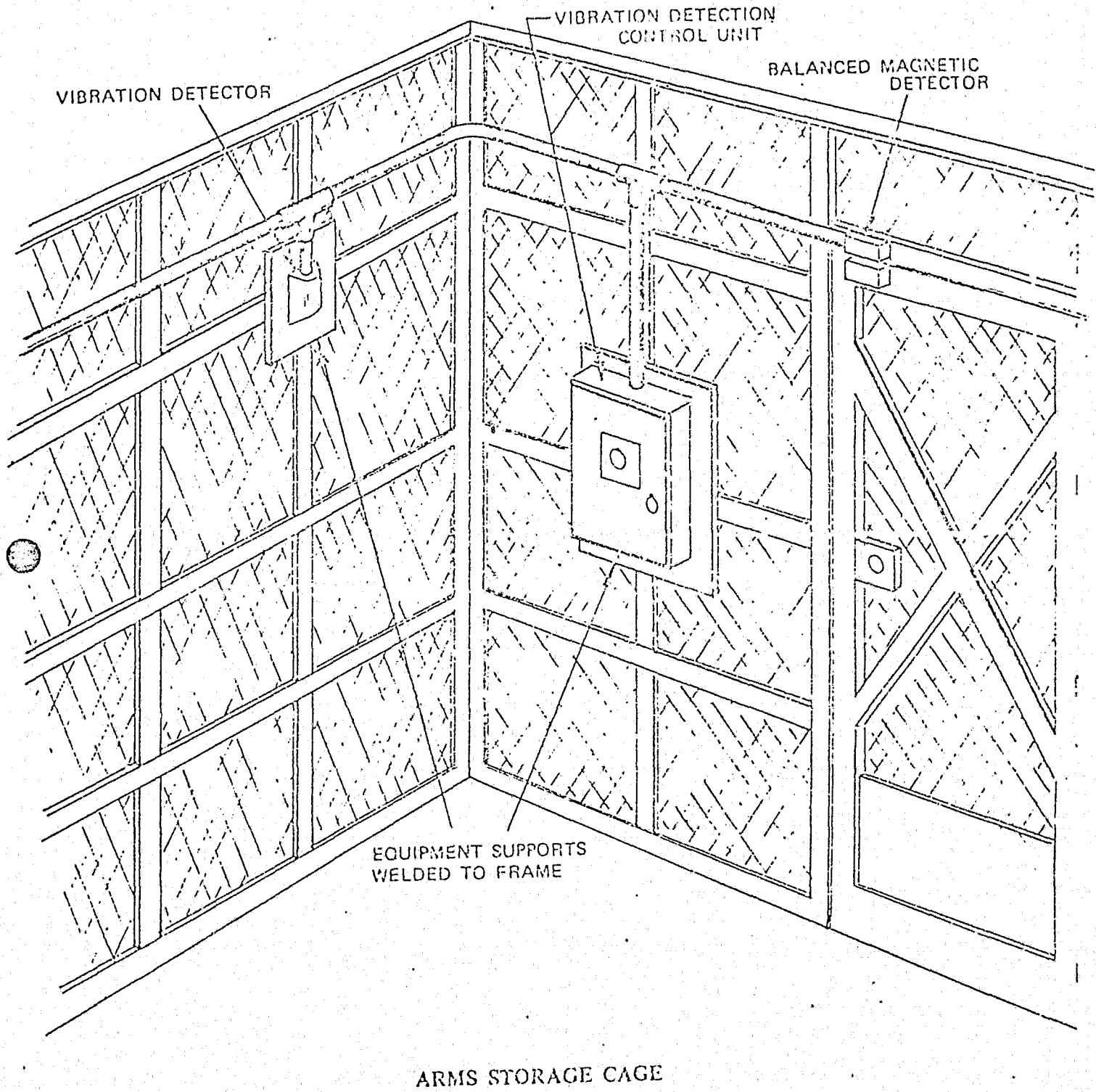


FIGURE 20

CONTINUED

1 OF 2

ARMS STORAGE AND SECURITY CABINETS

CAPACITANCE DETECTOR

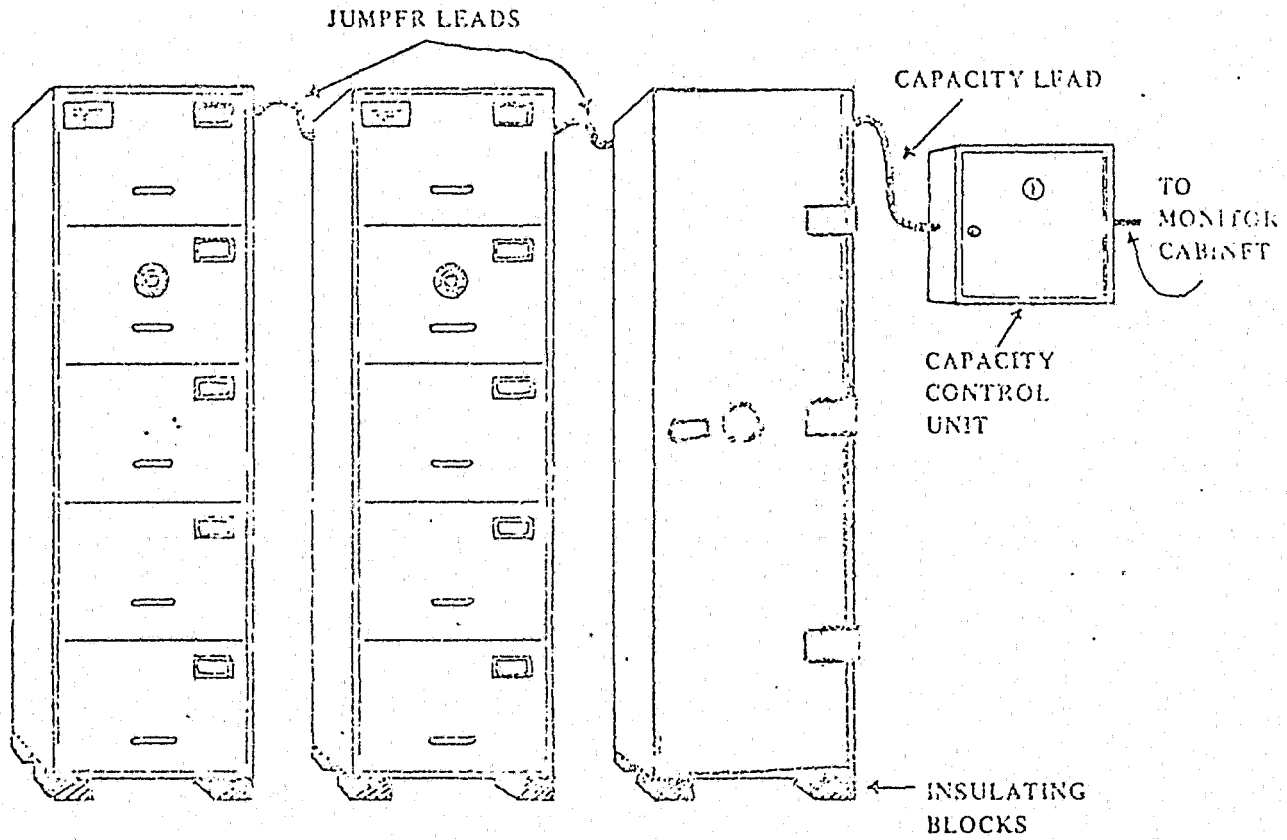


FIGURE 21

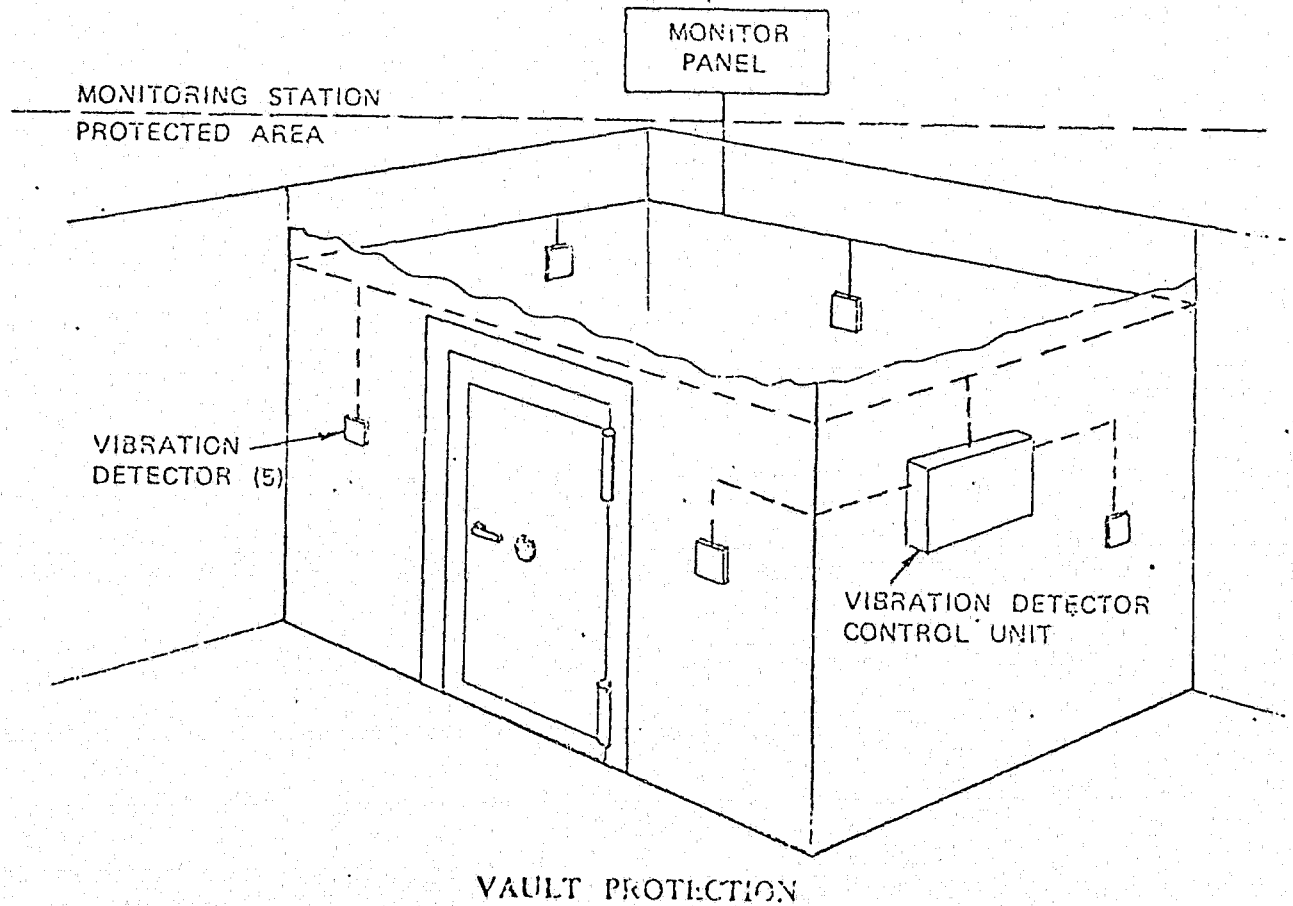
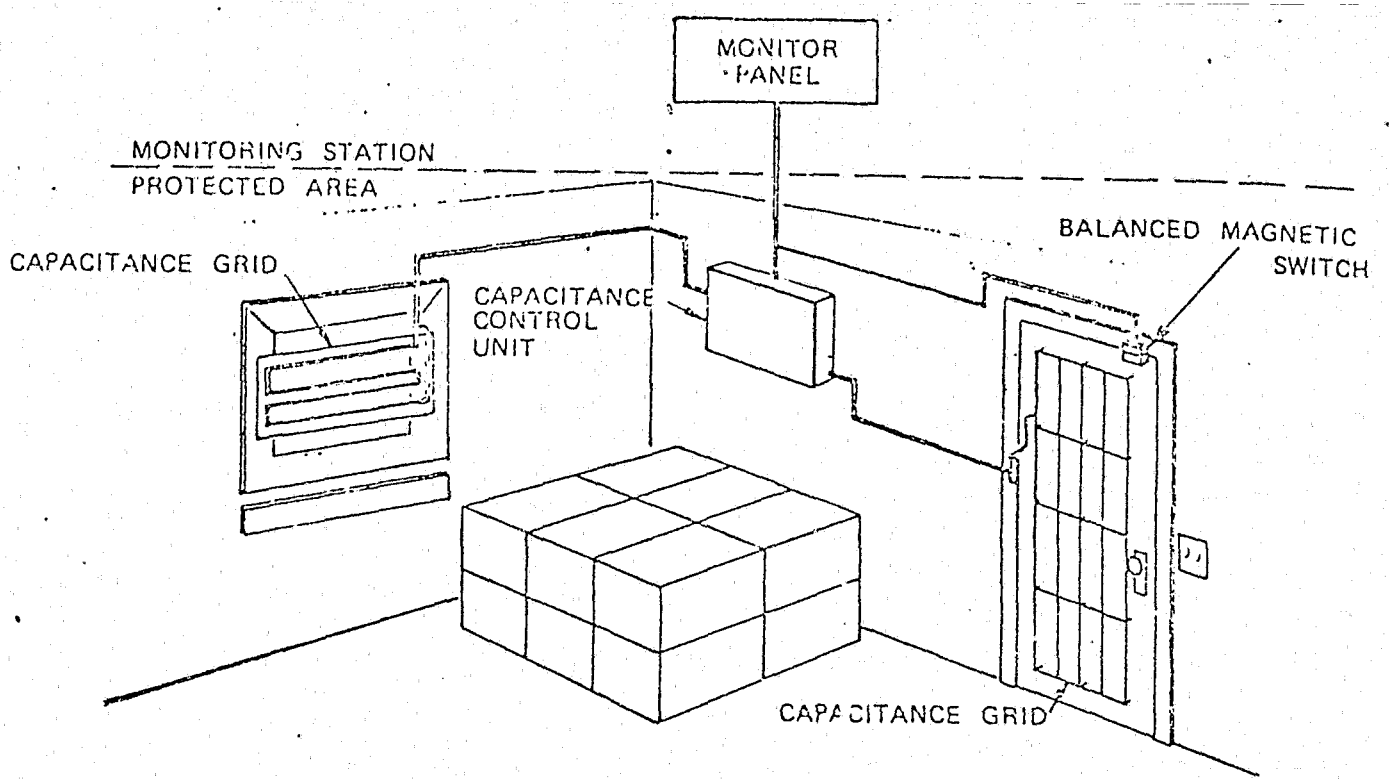
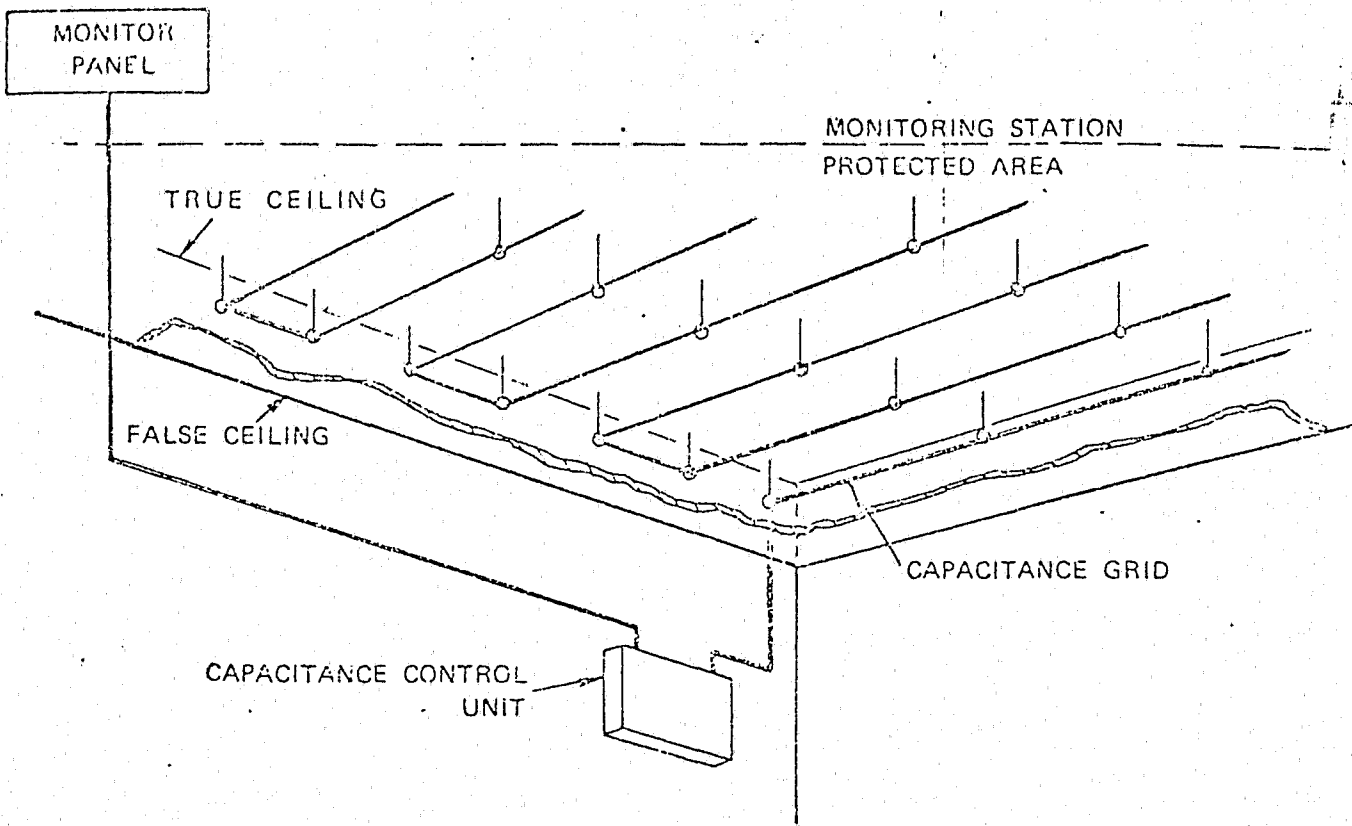


FIGURE 22



DEAD SPACE PROTECTION (Above False Ceilings)

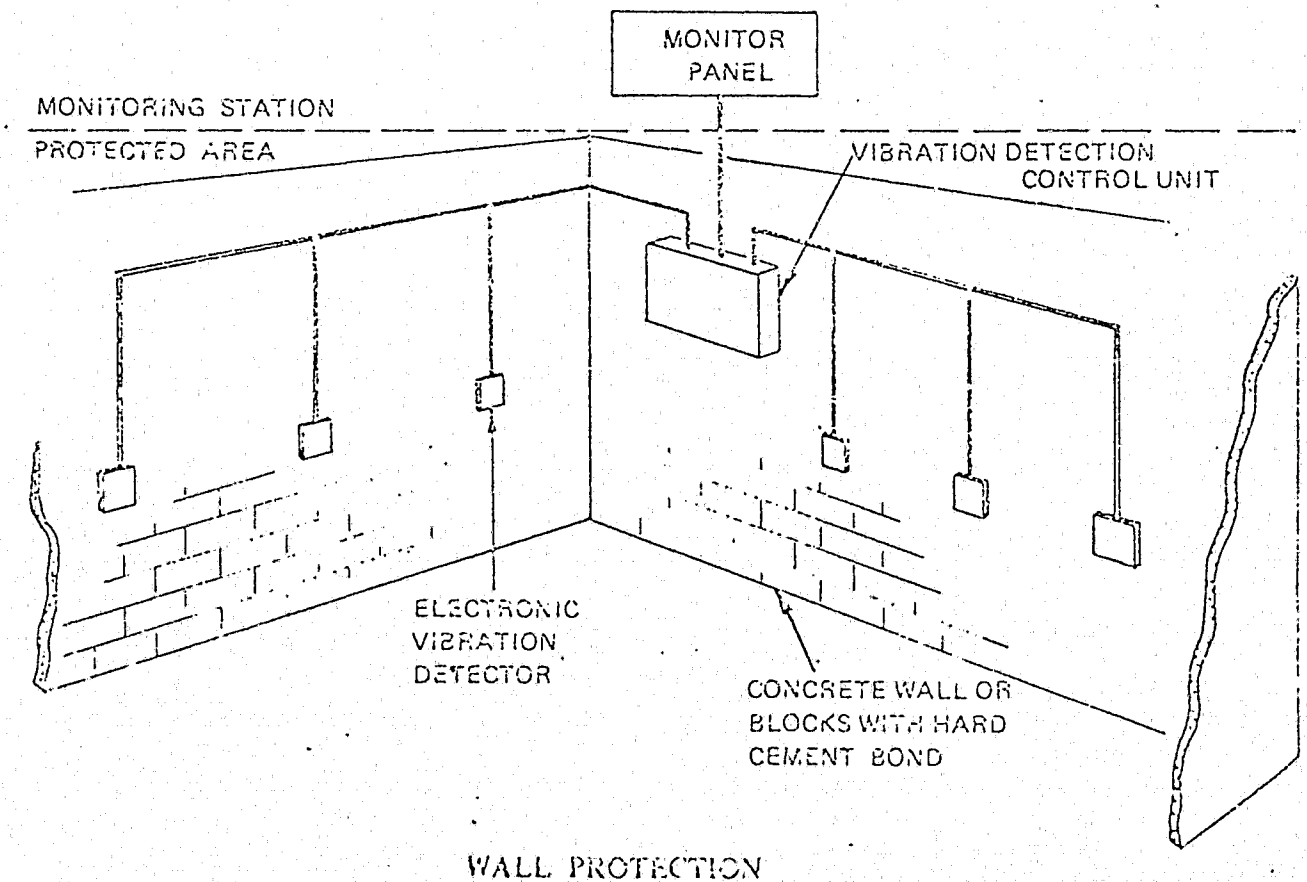
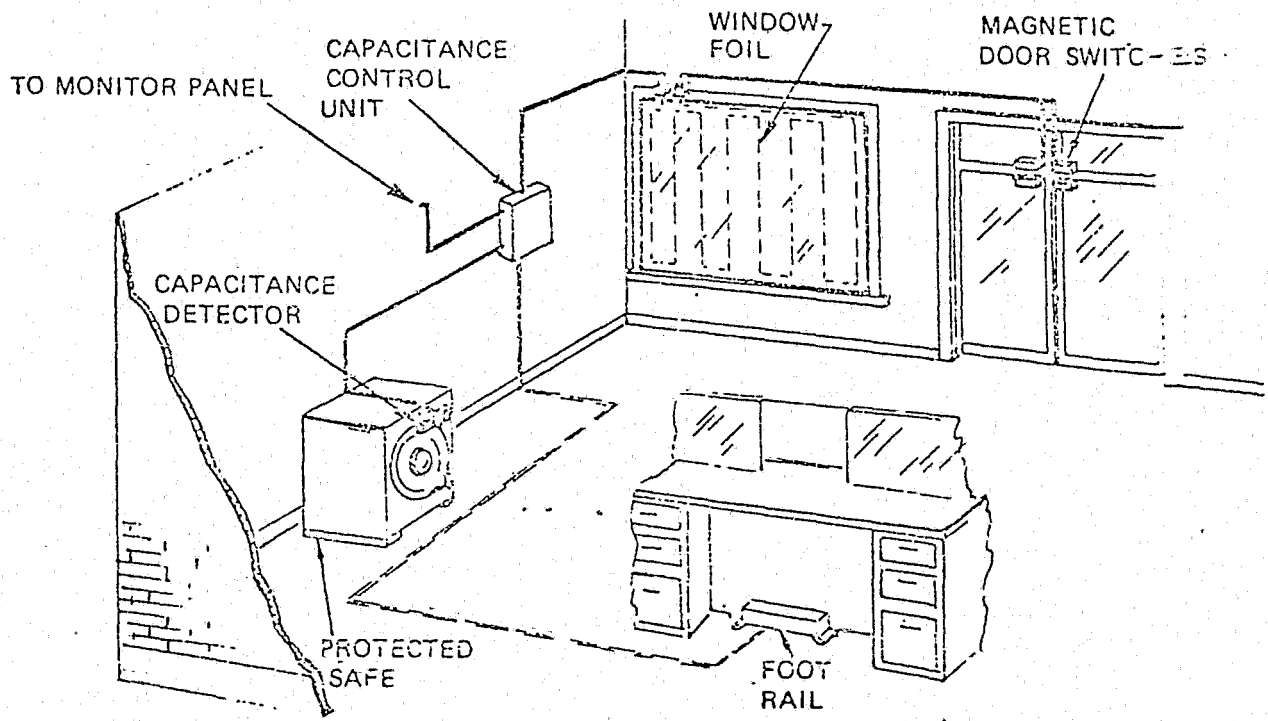


FIGURE 23



FINANCE DISBURSING OFFICE

FIGURE 24

Section III
FACILITY SURVEY

1. GENERAL: Intrusion detection alarm devices, systems and equipment are similar to fire alarms, sprinkler systems, safety alarms and other intangible integrals of a facility in their relation to engineering economics and justification. Such alarm systems serve to protect life and property and contribute to the preservation of productive capabilities, essential resources, and defense posture in a manner not necessarily proportional to the tangible cost of the facilities to which they are attached. The cost of alarm systems should be evaluated in relation to the expendability of the materiel resources they are employed to protect, rather than the replacement cost of the building structure or object in which they are installed. Due to either the intangibility of the protected resources, or the value of materials to be stored, the cost of the building or structure may have an inverse relationship to the cost of the alarm system best suited to the situation. Usually, in temporary buildings, economical physical barriers or substandard containers will require more sophisticated and reliable alarm systems than would be necessary for more durable facilities with some inherent protective features. The practice of some planners to promote a fixed percentage of budgeted cost of proposed facility for alarm systems and other security features, without due regard to intangibles and probable inverse cost relationships, is inimical to economical security operations. The similarity between intrusion

detection alarms and all other types of alarm systems is somewhat limited to economic justification, technical practices and fundamental concepts. There is one predominant factor which differentiates an intrusion detection system from any other type of alarm system, e.g., the incentive that exists for surreptitious compromise or covert disablement of the system and the benefits that could be derived from such a criminal activity.

1.1. UTILIZATION: The decision of whether or not to employ intrusion detection systems for any given security interest can be made by analysis of basic considerations, such as:

1.1.1. Availability of guards or other designated personnel to respond to alarms and to take appropriate protective actions.

1.1.2. Availability of alarm systems or equipment to meet the needs of the local situation.

1.1.3. Advantages, in cost, availability and operating convenience, of an alarm system over other physical security measures which could be employed for the security interests.

1.1.4. The necessity for providing supplemental aids or adjuncts for guard forces where physical barriers are not adequate or cannot be utilized.

1.1.5. Security operations and efficiency would be enhanced to a degree commensurate with the cost of providing, operating, and maintaining a suitable alarm system.

1.1.6. The local environment and occupancy of the premises are compatible with alarm system performance characteristics.

1.1.7. Duration of the requirement, life expectancy of the system or flexibility of the equipment to be procured will be such as to warrant the expenditure of funds required.

1.1.8. Precautions that excessive and unnecessary security measures are eliminated or reduced to realistic and practicable levels of security risks.

1.2. SCOPE: The determination of the complexity, sophistication, and multi-purpose utilization of supplemental features and components are the most difficult decisions faced by the planners and designers of intrusion alarm systems. Whether to include communications, access controls, exit controls, and visual surveillance of protected resources in the intrusion detection alarm system, or to design separate systems, is largely a matter of engineering economics best left to the qualified designer. However, the need of justification for such features should be determined by the cognizant security officer. Generally, it will be more economical to design a complete complementary security system for a new facility complex, new weapons system, or new storage facility. However, it may be less expensive to add detection systems appropriate for the local security interests on the basis of individual requirements at existing facilities. The installation of separate systems should not be construed as offering support for hodge-podge equipment of questionable compatibility or piece-meal procurement of partial systems. Each system

particularly those intrusion detection alarm systems for sensitive installations should be of comprehensive design to include all essential features, parts and components required for the specific service. Acquisition should be completed in a single procurement action to insure compatibility of characteristics and standardization of component parts.

2. PERFORMANCE FACTORS:

2.1. CHARACTERISTICS: The performance characteristics to be required of an intrusion detection system must be designed in relation to the environments under which it will be operated. There is no one system that will satisfy all requirements. Each type of detector, annunciator and signal circuit has been designed for certain intended applications and has proven satisfactory within known limits. It is essential that environmental conditions be stated, concise objectives and intended utilization be expressed, and performance characteristics be specified if maximum design efficiency is to be realized.

2.1.1. ENVIRONMENT: The environmental data required for design of intrusion alarm systems or selection of detection media will include the following:

2.1.1.1. Temperature (average and high-low extremes),

2.1.1.2. Noise level (ambient and extreme),

2.1.1.3. Wind loading (air velocities and continuity for indoor systems - maximum velocity for outdoor systems),

2.1.1.4. Vibration level (ambient, extreme, and extraneous influences to be tolerated),

2.1.1.5. Rainfall (maximum intensity for outdoor systems),

- 2.1.1.6. Snow cover (with applicable outdoor systems),
- 2.1.1.7. Electromagnetic Field (operating frequencies, amplitude and magnetic field strength of other equipment),
- 2.1.1.8. Frequency Allocation (for RF doppler systems),
- 2.1.1.9. Unusual conditions (any extreme condition not usually associated with the type of facility) and,
- 2.1.1.10. Light intensity (day and night - minimum and maximum for optical or image systems).

2.1.2. SUPPORT FACILITIES: The type of construction to be supported or supplemented and the availability of utilities to support the alarm system should be recorded. Information needed will include:

- 2.1.2.1. Power supply (voltage, frequency, phase, and distribution),
- 2.1.2.2. Cable facilities (existing or future telephone or other signal circuits to be used or furnished for alarm transmission),
- 2.1.2.3. Construction (type of fence, barriers, walls, roof, floor, etc.),
- 2.1.2.4. Openings (number and type of gates, doors, windows, vents, etc.),
- 2.1.2.5. Space (area or volume to be covered, and
- 2.1.2.6. Description (plans, drawings, or pictures showing details of features).

2.1.3. EXPOSURE: System exposure to unauthorized personnel will influence design of tamper resistance, test features, component construction and locations. Other important data includes:

- 2.1.3.1. Classification (clearances required for designers, installers, servicing, etc.),
- 2.1.3.2. Cable circuits (description of type, gate, aerial, underground, encasement, routing, commercial or proprietary),

2.1.3.3. Wiring (requirements for internal wiring-conduit, concealed, exposed, tampered, etc.),

2.1.3.4. Location (describe or show location of principle components), and

2.1.3.5. Personnel (technical competence and reliability of personnel who will operate and support the alarm system.

2.2. RELIABILITY: The reliability of the intrusion detection alarm system is its true measure of worth. The required characteristics should be expressed in terms of performance, since the specifications are provided in Section IV. Some features and provisions that will influence the system reliability, and consequently of interest to the security officer, are:

2.2.1. Fail-safe - degree to which system performance need be self-supervising.

2.2.2. Tamper Resistance - degree of inherent supervision against tampering or surreptitious compromise.

2.2.3. Test Features - requirement for remote or local test, manual or automatic.

2.2.4. Service Cycle - mean time before failure (MTBF) operating hours between component replacement or major repairs - calculated.

2.2.5. Nuisance Alarms - Maximum number of nuisance alarms, false alarms or failures of any cause that can be accepted during a specific period of time, o.e., alarms per circuit per year.

2.2.6. Maintainability - ease of access for maintenance, componentization, modularity, level of competence, etc.

2.2.7. Orientation - training to be given operators and maintenance personnel

2.2.8. Instructions - Manuals and drawings, parts lists to be furnished.

2.2.9. Spare Parts - parts and special tools to be furnished with system (minimum 90 days supply).

2.2.10. Guaranty - period & conditions.

2.2.11. Supervision - installation supervision to be furnished by manufacturer or other competent authority.

2.2.12. Performance Tests - list tests to be performed prior to acceptance, including the detection factor.

2.3. UTILITY: The utility of an intrusion detection alarm system will be measured by the sum of its attributes (toward guard force efficiency) as weighed against the liabilities of cost and care. In a large measure, alarm systems can be evaluated from the degree of acceptance and confidence in the system exhibited by its attendants. For full utilization a system should have the following attributes:

2.3.1. Simplicity - easy to operate, understand and live with.

2.3.2. Motivation - alarm signals should be clear and concise, distinctive signals should be standardized and meaningful.

2.3.3. Continuity - continuous "full time" performance is essential - standby or emergency power should be specified to cover the maximum power outage of record or anticipated.

2.3.4. Convenience - all operating controls should be conveniently located and identified.

e. Flexibility - system should offer reasonable expansion and relocation capabilities for any changing needs.

3. FACILITY SURVEY:

3.1. Prior to the preparation of a procurement requirement for ID equipment, it is essential that a thorough examination be conducted of the premise to be protected as well as the surrounding environment in which it is located. The checklist (Appendix A) provides a basis for review by command designated technical personnel to insure that the ID system being

solicited to be most appropriate for the environment since each system has its capabilities and limitation. A primary factor in selecting the appropriate components to comprise the system to protect a given area is the environment of the protected area. Environment is considered to be both the structural characteristics of the protected area as well as its physical location in proximity to other activities in the adjacent areas. Since the detection signals emanating from motion detectors can penetrate soft construction materials, the degree of hardness of walls, floors, etc., are of primary concern. Requirements for motion detectors will vary, e.g., in some instances, the protection of vaults, like other secure areas, may require only the application of vibration detector on the walls and ceiling, plus magnetic switches as well as a heat detector on the doors.

3.2. The check sheet is provided for guidance. Should a using activity require advice on determining the adequacy of their proposed selection of equipment, the local engineering support office should be consulted. If this is not possible, a copy of the check list plus other pertinent data should be forwarded to one of the two DA laboratory facilities mentioned in paragraph 1b, Section VII, with a copy to the FMG, DA.

4. System Cost Estimates: An important item in planning for procurement and installation of intrusion detection equipment is the estimated costs for budget purpose and for comparison with proposed commercial solicitation during actual contract negotiations. The following estimates are based upon average 1969-70 procurement cost. Precise cost should be obtained locally:

<u>ITEM</u>	<u>COST</u>
Motion Detector - (Per zone, includes standby power for 20x20 ft coverage)	\$900.00 - 1,500.00
Ultrasonic (Single unit with control)	800.00
4 Pickup	100.00
Microwave (One detector)	750.00
Control Unit	250.00
Audio	1,000.00
Photo Electric (Single Pair to include transmitters/	1,000.00
Receiver/Access Secure Unit	800.00
Vibration - Control Unit	300.00
Vibration Detector	30.00
Capacitance - (Approximately 3 ducts)	700.00
Foil/Protective wiring	2.00 sq ft
Control Unit	75.00
Holdup Devices	
Push Button	150.00 \$50 ea addt'l
Foot Rail	175.00 1st unit 75.00 ea addt'l unit
Panels -	
Per Zone (Included Labor and Handwork hookup)	
Class A -	500.00
B -	175.00
C -	125.00

<u>ITEM</u>	<u>COST</u>
Console Monitor	
Single Zone	\$500.00
2-10 Zone	2,000.00
10-20 Zone	3,500.00
20-50 Zone	7,000.00 - 10,000.00
Wire	
Rigid Conduit	3.00 per foot (cost vary by size)
EMT	2.00 per foot
Single Open Run Plain Wire (Wire requests/cost must be considered on one pair basis per instrument between zone and panel)	.10 per foot
Emergency Power Indicator (Per Zone)	150.00
Event Recorder	
50 Zone	6,000.00
100 Zone	7,500.00
200 Zone	10,500.00
Telephone System	
Basic Unit - 10 Zone	1,500.00
10-50 Zone	4,500.00
Heat Detector (may be connected in conjunction w/ another control unit located in protection zone)	35.00 ea

(Above prices include 12 hours standby power)

Section IV

STANDARDS FOR INTERIOR INTRUSION
DETECTION EQUIPMENT

INDEX

Paragraph		Pages
1.	General Requirements	25
1.1.	Scope	25
1.2.	Type of System	25
1.3.	Design Concept	25
1.4.	Electronic Counter-measure (ECM) Vulnerability	26
1.5.	Standard Products	26
2.	Technical Requirements	26
2.1.	General	26
2.1.1.	Maintainability	27
2.1.2.	Interchangeability	27
2.1.3.	Soldering	27
2.1.4.	Workmanship	27
2.1.5.	Cleaning	27
2.1.6.	Finish	27
2.1.7.	Miscellaneous Materials	28
2.1.8.	Environmental Requirements	28
2.1.8.1.	Humidity	28
2.1.8.2.	Temperature	28
2.1.9.	Manufacturers Name Plates	28
2.1.10	Locks and Key Lock Switches	29
2.1.11	Relays	29
2.1.12	Equipment Housings and Cabinets	29

Paragraph		Pages
2.1.12.1..	Construction	29
2.1.12.1.1.	Exposed to Weather Locations	30
2.1.12.1.2.	Protected Locations	30
2.1.12.1.3.	Hazardous Locations	30
2.1.12.2.	Tamper Switches	31
2.1.13.	Power Supplies	31
2.1.14.	Remote Test	32
2.2.	Detection Devices	32
2.2.1.	Electro-Mechanical Devices	32
2.2.1.1.	Access/Secure Control Unit	32
2.2.1.1.1.	Enclosures	32
2.2.1.1.2.	Power Supply	32
2.2.1.2.	Magnetic Switch	32
2.2.1.2.1.	Simple Magnetic Switch	33
2.2.1.2.1.1.	Enclosure	33
2.2.1.2.1.2.	Performance	33
2.2.1.2.2.	Balanced Magnetic Switches	33
2.2.1.2.2.1.	Enclosures	33
2.2.1.2.2.2.	Performance	34
2.2.1.3.	Foil	34
2.2.1.4.	Protective Wiring	34
2.2.1.5.	Hold-up Devices	35
2.2.1.5.1.	Push Button	35

Paragraph		Pages
2.2.1.5.2.	Foot Rails	35
2.2.1.6.	Heat Detectors	35
2.2.2.	Photo-Electric System	35
2.2.2.1.	Transmitter Unit	36
2.2.2.2.	Receiver Unit	36
2.2.2.3.	Access/Secure Control Unit	36
2.2.2.3.1.	Enclosure	36
2.2.2.3.2.	Power Supply	36
2.2.2.4.	Performance	36
2.2.3.	Vibration Detection Systems	37
2.2.3.1.	Vibration Detection	37
2.2.3.1.1.	Enclosures	38
2.2.3.1.2.	Power Supply	38
2.2.3.1.3.	Remote Test	38
2.2.3.2.	Vibration Sensor	38
2.2.3.3.	Performance	38
2.2.4.	Audio Detection System	39
2.2.4.1.	Audio Detection Control Unit	39
2.2.4.1.1.	Enclosure	39
2.2.4.1.2.	Power Supply	39
2.2.4.1.3.	Remote Test	39
2.2.4.2.	Audio Sensor	39
2.2.4.3.	Performance	40

Paragraph		Pages
2.2.5.	Capacitance Detection System	40
2.2.5.1.	Capacitance Control Unit	40
2.2.5.1.1.	Enclosure	40
2.2.5.1.2.	Power Supply	41
2.2.5.1.3.	Remote Test	41
2.2.5.2.	Capacitance Sensors	41
2.2.5.3.	Performance	41
2.2.6.	Motion Detection Systems	41
2.2.6.1.	Enclosure	41
2.2.6.2.	Power Supply	41
2.2.6.3.	Remote Test	41
2.2.6.4.	Performance	41
2.2.6.5.	Ultrasonic Motion Detection System	42
2.2.6.5.1.	Ultrasonic Control Unit	42
2.2.6.5.2.	Ultrasonic Sensors	43
2.2.6.6.	Microwave Motion Detection System	43
2.2.6.6.1.	Microwave Control Unit	43
2.2.6.6.2.	Microwave Sensors	43
2.3.	Monitoring Facilities	44
2.3.1.	Monitor Panels	44
2.3.1.1.	Visual Indicators	44
2.3.1.1.1.	Labeling	44
2.3.1.1.2.	Colors	44

Paragraph		Pages
2.3.1.1.2.1.	Red	44
2.3.1.1.2.2.	Yellow	44
2.3.1.1.2.3.	Green	44
2.3.1.1.3.	Arrangement	44
2.3.1.1.4.	Signal Lamps	45
2.3.1.2.	Audible Signalling Devices	45
2.3.1.3.	Access/Secure Function	46
2.3.1.4.	Reset Function	46
2.3.1.5.	Alarm Function	47
2.3.1.6.	Remote Test Function	47
2.3.1.7.	Line Supervision	47
2.3.1.7.1.	Class "A" Supervision	47
2.3.1.7.2.	Class "E" Supervision	48
2.3.1.7.3.	Class "C" Supervision	49
2.3.1.8.	Alarm Transmission Lines	49
2.3.1.9.	Interchangeability	49
2.3.1.10.	Front Panel Components	49
2.3.2.	Emergency Power Indicators	49
2.3.2.1.	Visual Indicators	49
2.3.2.1.1.	Labeling	49
2.3.2.1.2.	Colors	50

Paragraphs		Page
2.3.2.1.2.1.	Amber	50
2.3.2.1.2.2.	Green	50
2.3.2.1.3.	Arrangement	50
2.3.2.1.4.	Signal Lamps	50
2.3.2.2.	Audible Signalling Devices	51
2.3.2.3.	Alarm Function	51
2.3.2.4.	Test Function	52
2.3.2.5.	Line Supervision	52
2.3.2.6.	Alarm Transmission Lines	52
2.3.2.7.	Interchangeability	52
2.3.2.8.	Front Panel Components	52
2.3.3.	Event Recorder	52
2.3.3.1.	Controls	53
2.3.3.2.	Power Supply	53
2.3.3.3.	Emergency Power Indicator	54
2.3.3.4.	Mounting	54
2.3.3.5.	System Capacity	54
2.3.3.6.	Option	54
2.3.4.	Security Communications Systems	54
2.3.4.1.	Operation	55
2.3.4.2.	Power Supply	55

Paragraphs		Pages
2.3.5.	Monitor Cabinet	55
2.3.5.1.	Layout and Arrangement	55
2.3.5.2.	Enclosure	56
2.3.5.3.	Power Supply	56
2.3.5.4.	Emergency Power Indicator	56
2.3.5.5.	Remote Signalling	56

SECTION IV

STANDARDS FOR INTERIOR INTRUSION DETECTION EQUIPMENT

1. GENERAL REQUIREMENTS:

1.1 SCOPE: This specification covers the requirements for Interior Intrusion Detection Equipment and is intended for use in procurements involving Interior Intrusion Detection Systems.

1.2 TYPE OF SYSTEM: The Interior Intrusion Detection Equipment described in this specification is of the proprietary or central type designed to transmit signals automatically over electrically supervised lines from detectors installed in protected areas to a monitor facility located in the monitoring area.

1.3 DESIGN CONCEPT: Design of the Interior Intrusion Detection System and its components shall be basically conservative to insure that the system is inherently stable, defeat-resistant, fail-safe, durable, reliable, and suitable in every respect for satisfactory, long lasting, and continuous operation. The design shall be such that it will require a minimum of maintenance and adjustments. The system shall not have more than one nuisance alarm per week from the entire system during continuous 24 hour a day operation under all normal variations of use conditions. In addition, the system shall be so designed that an alarm will be initiated when any circuit, power supply, or component fails or ages to such an extent as to nullify the effectiveness of the system. Restoration to normal operation shall not be possible until the fault is corrected.

1.4 ELECTRONIC COUNTERMEASURE (ECM) VULNERABILITY: Interior Intrusion Detection Equipment shall be so designed and constructed as to provide maximum practicable invulnerability to electronic countermeasure action. Techniques and circuits utilized shall be those which will more effectively reduce the vulnerability to countermeasures.

1.5 STANDARD PRODUCTS: All materials and equipment in the Interior Intrusion Detection System shall be new and of standard design or model, the products of manufacturers regularly engaged in the production of such equipment. In addition, they shall be the manufacturers' latest standard designs current at the time of delivery, except for such modifications from manufacturers' standards as may be required to conform to specification requirements. Where two or more units of the same class of equipment are required, such units shall be the standard products of a single manufacturer, but all of the component parts of the system need not be the products of the same manufacturer. Manufacturers shall be so established in the industry that prompt and continuing service and delivery of spare parts may be assured.

2. TECHNICAL REQUIREMENTS: Interior Intrusion Detection Systems furnished under this specification shall comply with the following technical requirements:

2.1 GENERAL: All components of the system shall, as a minimum, conform to the following general requirements:

2.1.1 MAINTAINABILITY: Devices and equipments shall be designed and constructed to facilitate modular, unitized, component replacement to the maximum extent feasible. Components shall be so arranged and assembled that they are readily accessible to maintenance personnel without compromising the defeat-resistance of the system. Controls and adjustments inside enclosures, requiring manipulation by maintenance personnel, shall be readily visible and accessible with minimum disassembly of the equipment.

2.1.2 INTERCHANGEABILITY: Like units, assemblies, sub-assemblies, and replaceable parts shall be physically and functionally interchangeable as complete items, without modification thereof, or of other articles with which the items are used. Individual items shall not be hand-picked for fit or performance. Reliance shall not be placed on any unspecified dimension, rating, characteristic, etc. Subassemblies and parts shall be readily replaceable in the field.

2.1.3 SOLDERING: Soldering shall be consistent with the best commercial practice.

2.1.4 WORKMANSHIP: Workmanship shall be consistent with the best commercial practice.

2.1.5 CLEANING: After fabrication, parts shall be cleaned in accordance with best commercial practice. Cleaning processes shall not have any detrimental effect upon operation of the system.

2.1.6 FINISH: All exposed surfaces of devices, component enclosures, cabinets, and other items of equipment shall be

thoroughly cleaned, and shall be dry and free from all scale, oil, grease, dirt, and rust; also, those surfaces shall be painted as soon as practicable after cleaning. Ferrous surfaces shall have a rust-inhibiting primer, after which all surfaces shall be provided with not less than two coats of synthetic enamel or baked-on enamel. Primer and finish coats shall be applied in accordance with approved commercial practices to assure complete coverage and durability of the finish. The finish coat, when dry, shall be an even surface, free from runs, sags, or other blemishes. Unless otherwise specified, exposed surfaces shall be of the manufacturers' standard color.

2.1.7 MISCELLANEOUS MATERIALS: All materials and components not definitely specified herein shall be of the best quality used in the manufacturers' normal commercial products. Materials and components shall be free from defects and imperfections that effect the safety, serviceability, and defeat-resistance of the finished product.

2.1.8 ENVIRONMENTAL REQUIREMENTS: All components shall be capable of full operation under the following conditions:

2.1.8.1 HUMIDITY: Up to 85 percent relative humidity.

2.1.8.2 TEMPERATURE: Any ambient temperature in the range from +32 degrees F. to +120 degrees F.

2.1.9 MANUFACTURERS NAME PLATES: Each major component of the system shall have the manufacturer's name, address, name and

catalog number of the component, indented or embossed on a name plate securely affixed to the unit. This label shall be affixed in such a manner as to prevent identification of the unit without removing the cover or opening the door.

2.1.10 LOCKS AND KEY LOCK SWITCHES: All lock and key-lock switches required to be installed in the system shall be of the round key "ACE" type. All key lock switches shall be keyed differently and two keys furnished for each switch. All locks on equipment and power supply enclosures for maintenance access shall be keyed alike and two keys furnished for the entire system. The contractor shall exercise every precaution to protect the security of these keys. Upon completion of the work, the keys, properly tagged, shall be delivered to the contracting officer.

2.1.11 RELAYS: Light-duty relays and similar devices shall have dust covers which protect against fouling by dust or other material which may adversely affect their normal operation.

2.1.12 EQUIPMENT HOUSINGS AND CABINETS: Equipment housings and cabinets shall conform to the following requirements:

2.1.12.1 CONSTRUCTION: Enclosures for monitor panels, power supplies, terminal cabinets, detection equipment and other system components shall be so formed and assembled as to have ample strength and rigidity necessary to resist the abuses to which they are likely to be subjected. They shall be constructed of sheet steel and shall be not less than No. 16 U.S. Standard Gage. Enclosures shall not have prepunched knockouts.

Where doors are mounted on hinges with exposed pins, the hinges shall be tack welded to prevent ready removal. The latch edge of movable covers or doors shall be equipped with a lock which meets the requirements of paragraph 2.1.10. of this specification. Where the latch edge of a movable cover or door is 24" or more in length, the door shall be provided with two locks, which meet the requirements of paragraph 2.1.10 of this specification, one located near each end. Any ventilator openings in enclosures and cabinets shall be protected by internal baffling. All doors shall be flanged to prevent ready access to the interior of the enclosure until the tamper device has actuated.

2.1.12.1.1. EXPOSED TO WEATHER LOCATIONS: Enclosures for use in exposed-to-weather locations, shall be of weatherproof construction which is suitably protected against corrosion. Any unused threaded holes or hubs shall be closed with threaded plugs which cannot be surreptitiously removed from outside the enclosure or fitting.

2.1.12.1.2. PROTECTED LOCATIONS: Unless otherwise specified, enclosures for use in areas which are protected from the weather shall be mounted in general purpose enclosures as described above.

2.1.12.1.3. HAZARDOUS LOCATIONS: Enclosures for use in hazardous locations shall comply with applicable articles, clauses, groups, and division of the National Electrical Code.

2.1.12.2 TAMPER SWITCHES: Enclosures shall be provided with cover-operated, corrosion-resistant tamper switches arranged to actuate an alarm signal when the door or cover is moved as much as 1/4" from its normally closed position. The tamper switch shall remain inaccessible until it has activated. Tamper switch mounting hardware shall be concealed so that location of the switch cannot be visually detected from the exterior of the enclosure. Tamper switches shall remain under supervision at all times, whether the circuit in which they are installed is in the authorized "Access", or "Secure" mode. Tamper switches on doors which must be opened to make normal maintenance adjustments to the system and service the power supplies, shall be of the push, pull-set, automatic reset type.

2.1.13 POWER SUPPLIES: Power supplies shall operate normally on AC power supplied at the protected area, and shall be capable of stable operation if the supply voltage varies between 102 and 132 VAC and/or the frequency varies between 58 and 62 Hz. A battery shall be provided to operate the system for a period of 12, 24, 36, or 48 hours whichever is specified in the system requirements. The battery shall be of the sealed nickel-cadmium, lead acid, or "Gel Cell" type. The power supply shall be so arranged that:

2.1.13.1 The battery is maintained fully charged at all times when AC power is available.

2.1.13.2 The battery is fully recharged within 48 hours after any period of battery operation.

2.1.13.3 Detectors automatically transfer from AC power to battery power whenever the former fails, and returns to AC

power upon restoration of that power.

2.1.13.4. Alarms are not initiated upon transfer from one power source to another.

2.1.13.5. Provisions shall be made to provide a signal which may be used in the monitor cabinet to indicate loss of AC power.

2.1.14. REMOTE TEST: Detection equipment shall have the capability of being remotely tested from the monitor cabinet.

2.2. DETECTION DEVICES: Detection devices shall comply with the following requirements:

2.2.1. ELECTRO-MECHANICAL DEVICES: Electro-mechanical devices shall provide an alarm signal when the electrical continuity of the devices are interrupted.

2.2.1.1. ACCESS/SECURE CONTROL UNIT: Electro-mechanical devices shall be equipped with an Access/Secure Control unit to provide the proper line termination for the monitor system, and any power required by the device.

2.2.1.1.1. ENCLOSURES: The enclosure shall comply with the requirements of paragraph 2.1.12 of this specification.

2.2.1.1.2. MAGNETIC SWITCH: The magnetic switch shall operate when a magnetic field is brought in close proximity. In addition, switches shall be of the Hermetically Sealed, Reed type which shall withstand a minimum of 50,000 activations without failure.

2.2.1.2.1 SIMPLE MAGNETIC SWITCH: The simple magnetic switch shall be of the type which opens and crosses or opens and grounds the circuit when activated.

2.2.1.2.1.1 ENCLOSURE: The switch and magnet shall be enclosed in an unsupervised housing of plastic, cast nonferrous metal, or any material providing reasonable protection against water, dust, etc.

2.2.1.2.1.2 PERFORMANCE: Simple magnetic switches shall be mounted so an alarm is initiated whenever the latch or lead edge of the enclosure on which it is mounted is moved as much as two inches from its closed position.

2.2.1.2.2 BALANCED MAGNETIC SWITCHES: The balanced magnetic switch shall be of the type which opens and crosses, or opens and grounds the circuit when actuated. The switch mechanism shall be of the balanced magnetic type. It shall initiate an alarm upon increase, decrease, or attempted substitution of a magnetic field applied to the switch when in the normally secured position. The mechanism shall be internally adjustable so that the operating gap between faces of the switch housing and the magnet housing may be adjusted from 1/4" to 1" to accommodate installation variances. The switch shall be protected to prevent damage of its contacts from voltage or current surges.

2.2.1.2.2.1 ENCLOSURES: Switch and magnets shall be housed in weather proof boxes cast of nonferrous metal. Switch boxes shall be of the hub type, or shall have threaded bodies. The cover of the magnet housing shall not be readily

removable. Covers of cast aluminium switch boxes shall be secured by stainless steel screws. The switch boxes shall have flanges cast into the housing which prevent access to the interior of the housing until the tamper switch has activated. Tamper switches shall comply with the requirements of paragraph 2.1.12.2 of this specification.

2.2.1.2.2.2 PERFORMANCE: Balanced magnetic switches shall be mounted so an alarm is initiated whenever the latch or lead edges of the enclosure is moved as much as one inch from its closed position.

2.2.1.3 FOIL: Foil shall not exceed 1.2 pounds in tensile strength and shall be capable of carrying a minimum current of 60 milliamperes at 60 volts with a temperature rise of not more than one degree centigrade. Foil shall not exceed 1/2" in width for the protection of glass panes, or one inch in width for protection of opaque barriers such as walls, partitions, and door surfaces other than glass panels. Adhesives and coating materials shall be resistant to aging, moisture, and temperature change. The performance of the foil shall require that it initiate an alarm signal whenever circuit continuity is interrupted.

2.2.1.4 PROTECTIVE WIRING: Protective wiring shall not exceed 4.0 pounds in tensile strength, and shall be capable of carrying a maximum of 60 milliamperes at 60 volts with a temperature rise of not more than one degree centigrade. Wiring shall be no longer than 30 AWG. The wiring shall be continuous with no splices from one connecting point to another.

The performance of the protective wiring shall require that it initiate an alarm condition whenever the protective wiring circuit continuity is interrupted.

2.2.1.5 HOLD-UP DEVICES: Hold up devices shall actuate an alarm signal when operated, and shall lock in the signal until manually reset with a key or similar device.

2.2.1.5.1 PUSH BUTTON: Push button devices shall consist of a housing which protects the device from accidental activation, and push button which may be easily operated in an unobtrusive manner.

2.2.1.5.2 FOOT RAILS: Foot rails must be reliable, easy to operate, and securely mounted in a rugged corrosion resistant housing. The foot rail must be designed to minimize nuisance alarms, yet permit unobtrusive operation. In addition, once the foot rail has been activated, it can only be reset by the use of a key.

2.2.1.6 HEAT DETECTORS: Heat detectors shall be of the automatic reset type and shall actuate an alarm when the temperature rises above a preset level or as the temperature increases at a rate which is faster than a preset rate. The detector unit shall cause an alarm when the ambient temperature exceeds 135 degrees F. and/or the rate of rise of temperature exceed 5 degrees F. in 20 seconds.

2.2.2 PROTO-ELECTRIC SYSTEM: Photo-Electric systems shall consist of a transmitter, receiver, and an Access/Secure unit with power supply. The system shall be of the type employing a

modulated infra-red beam. The system shall operate satisfactorily with separation of up to 300 feet between the transmitter and receiver units.

2.2.2.1 TRANSMITTER UNIT: The transmitter unit shall utilize a pulsed or modulated solid state infra-red emitting diode, a lens to shape the light beam, and a device to prevent lens fogging. The enclosure shall comply with the requirements of paragraph 2.1.12 or paragraph 2.2.2 of this specification.

2.2.2.2 RECEIVER UNIT: The receiver unit shall include a lens to match that of the transmitter unit, a photodiode, alarm logic circuitry, and a device to prevent lens fogging. The enclosure shall comply with the requirements of paragraph 2.1.12 or paragraphs 2.2.2 and 2.2.2.1 of this specification..

2.2.2.3 ACCESS/SECURE CONTROL UNIT: The Access/Secure Control Unit shall provide the proper termination for the monitor system.

2.2.2.3.1 ENCLOSURE: The enclosure shall comply with the requirements of paragraph 2.1.12 of this specification.

2.2.2.3.2 POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2.1.13 of this specification.

2.2.2.4 PERFORMANCE: An alarm signal shall be initiated whenever the beam is completely intercepted. To prevent nuisance alarms due to smoke, fog, snow, or similar attenuating conditions,

the system shall be designed so that up to 95 percent of the beam may be intercepted without causing an alarm.

2.2.3 VIBRATION DETECTION SYSTEMS: The vibration detection system shall consist of one or more sensitive selectronic pick-up devices mounted on the surface(s) of walls, ceilings, and/or floors designated to be protected and connected through an amplifier/accumulator designed to initiate an alarm signal in response to stimuli of the types herein described.

2.2.3.1 VIBRATION DETECTION: The vibration detection control unit shall contain an amplifier which shall be of the low band pass type, and shall have included therein an impulse accumulator employing a resistance-capacitance time constant accumulator; a stepping relay, or other means to integrate the amplitude of input signals with respect to amplitude and time. The intergration circuit shall be so designed that an alarm signal shall be initiated in response to an explosion or a single heavy blow, or a series of lighter blows. In addition, the accumulator shall be so designed that stimuli of insufficient magnitude to initiate an alarm are bled off to the normal zero level at a rate of decay from the level immediately below alarm to zero in not less than 10, or more than 30 minutes. The amplifier accumulator shall have an adjustable gain control and an adjustable accumulator control. The controls shall be housed inside the vibration detector control unit enclosure, accessible only to maintenance personnel.

2.2.3.1.1. ENCLOSURES: The enclosure shall comply with the requirements of paragraph 2. 1. 12. of this specification.

2.2.3.1.2. POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2. 1. 13. of this specification.

2.2.3.1.3. REMOTE TEST: The remote test function shall comply with the requirements of paragraph 2. 1. 14. of this specification.

2.2.3.2. VIBRATION SENSOR: Vibration sensors shall be of the Piezoelectric or reluctance type designed to give peak response to structurally-conveyed vibration frequencies which would be associated with a forcible attack upon the solid body to which they are attached. The vibration sensor shall contain a pre-amplifier with adjustable gain control.

2.2.3.3. PERFORMANCE: The performance of this system shall be adjustable and is specified on the basis that the amplifier/accumulator with vibration sensors mounted on monolithic reinforced concrete block walls at least 6" thick, or hollow masonry concrete unit walls at least 8" thick, shall be capable of detecting and integrating so as to initiate an alarm signal whenever the protected slab or wall is struck on the exterior surface, within a minimum radius of 15 feet from a pickup device by five blows at two second intervals, from a one and one half pound hammer falling free through a 90 degree arc at a radius of 12". With the amplifier/accumulator adjustment controls set at minimum sensitivity, the system shall not respond to the foregoing hammer test beyond a radius of 10 feet from the pickup device.

2.2.4. AUDIO DETECTION SYSTEM: The audio detection system shall consist of one or more sensitive microphones mounted within an area to be protected and connected to an amplifier/accumulator designed to initiate an alarm signal in response to the stimuli of the types herein described.

2.2.4.1. AUDIO DETECTION CONTROL UNIT: The audio detection control unit shall contain an amplifier which shall be of the low band-pass type, and shall have included therein an impulse accumulator employing a resistance-capacitance time constant accumulator, a stepping relay, or other means to integrate the amplitude of input signals with respect to amplitude and time. The integration circuit shall be so designed that an alarm signal shall be initiated in response to a single loud sound, or a series of normal sounds. In addition, the accumulator shall be so designed that stimuli of insufficient magnitude to initiate an alarm are bled off to the normal zero level at a rate of decay from the level immediately below alarm to zero in not less than 10, or more than, 30 minutes. The amplifier/accumulator shall have an adjustable gain control, and an adjustable accumulator control. The controls shall be housed inside the audio detector control unit enclosure, accessible only to maintenance personnel.

2.2.4.1.1. ENCLOSURE: The enclosure shall comply with the requirements of paragraph 2. 1. 12. of this specification.

2.2.4.1.2. POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2. 1. 13. of this specification.

2.2.4.1.3. REMOTE TEST: The remote test function shall comply with the requirements of paragraph 2. 1. 14. of this specification.

2.2.4.2. AUDIO SENSOR: Audio sensors shall be of the Piezo-electric or reluctance type designed to give peak response to sound which

would be associated with authorized activity in a closed area in which they are installed. The audio sensor shall contain a preamplifier with an adjustable gain control. The enclosure shall comply with the requirements of paragraph 2.1.12 of this specification.

2.2.4.3. PERFORMANCE: Audio detection alarms shall activate in the protected area when:

2.2.4.3.1. There is a single sound of 65 decibels or more.

2.2.4.3.2. There is a series of five sounds of 45 decibels or more.

2.2.5. CAPACITANCE DETECTION SYSTEM: The capacitance detection system shall consist of a control unit which shall contain circuitry for detecting a change of the capacitance value to ground of an antenna or set of antennas. The antennas shall be energized to create an electrostatic or electromagnetic field, or that if they are approached or touched by a conductive mass of the density of a human body, whether grounded or ungrounded, the system will be unbalanced, and an alarm initiated.

2.2.5.1. CAPACITANCE CONTROL UNIT: The capacitance control unit shall be provided with authorized entry controls and shall be so designed that if the antennas have been tampered with during the period of ACCESS, the system will not reset upon restoration of the SECURE condition. The control unit shall supervise the continuity of the sensor loop as well as the capacitance load during the SECURE mode of operation. The control unit shall be constructed so the enclosure is not sensitive to touch. The capacitance control unit shall be capable of accepting an antenna load of at least 6,000 mmf. and still be adjustable over its sensitivity range.

2.2.5.1.1. ENCLOSURE: The enclosure shall comply with the requirements of paragraph 2.1.12 of this specification.

2.2.5.1.2. POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2.1.13 of this specification.

2.2.5.1.3. REMOTE TEST: The remote test function shall comply with the requirements of paragraph 2.1.14 of this specification.

2.2.5.2. CAPACITANCE SENSORS: Capacitance sensors shall be in the form of an ungrounded antenna array. Where grids or radiators are employed as antennas, they shall be insulated from ground, and shall be composed of nonferrous metal rods, tubes, or wires as best suited to the particular application. Wires used for grids shall not be smaller than NO 18 AWG. stranded. Elements of grids shall be spaced not more than 6" o.c. Grids shall be substantially protected and reflect neat, professional workmanship. When the object protected is a metal cabinet, chest, or safe, it shall be isolated from ground by insulating blocks and serve as the antenna element.

2.2.5.3. PERFORMANCE: Antennas shall be insensitive to movements of a human body at distances in excess of 36 inches from the radiator. Detectors shall respond to a human body in close proximity to the radiator. The distance shall be adjustable from contact to several inches.

2.2.6. MOTION DETECTION SYSTEMS: Motion detection systems shall detect the movement of a person within an area at a specified rate.

2.2.6.1. ENCLOSURE: The enclosure shall comply with the requirements of paragraph 2.1.12 of this specification

2.2.6.2. POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2.1.13 m., of this specification.

2.2.6.3. REMOTE TEST: The remote test function shall comply with the requirements of paragraph 2.1.14 of this specification.

2.2.6.4. PERFORMANCE: Design of the detection unit shall contain a sensitivity adjustment so that the system can be tuned to increase or decrease

overall detection sensitivity. Sensitivity shall be capable of being adjusted to respond to the movement of a person walking not more than four consecutive steps at a rate of one half (1/2) step per second. Such a four step movement shall constitute a trial, and a sufficient number of detection units shall be installed so that upon test, an alarm will be initiated in every trial made, moving progressively throughout the protected area.

2.2.6.5. ULTRASONIC MOTION DETECTION SYSTEM: The ultrasonic motion detection system shall be the detection of a Doppler shift of ultrasonic sound waves, activate an alarm signal when a person moves at a specified rate. Transmission and reception of all sound waves shall be by transmitters and receivers located within the protected area. The sound waves shall be of such nature that they will not penetrate walls, floors, or ceilings of the protected areas.

2.2.6.5.1. ULTRASONIC CONTROL UNIT: The detection circuits shall contain an oscillator which shall create a continuous tone signal. This tone signal shall be fed to the speaker transducers. The pickup transducers shall receive the tone signal and return it to the control unit. Movements within the protected area shall cause a change in the frequency of the received signal by the Doppler effect. Movements at the rate of, or greater than, those specified shall cause an alarm on the corresponding monitor panel. Controls shall be provided in the control unit to adjust the system sensitivity. The system shall have a fail-safe feature coupled with the system oscillator circuit which will activate an alarm signal in the event of intermittent or complete oscillator failure.

2.2.6.5.2 ULTRASONIC SENSORS: Pick-up and speaker transducers shall be of the Piezoelectric type. Sufficient transducers shall be installed in each system to meet the proper sensitivity requirements. The enclosure shall be of rugged construction with a corrosive resistant finish. The enclosure shall be equipped with a cover operated tamper switch which shall comply with paragraph 2.1.12 of this specification

2.2.6.6 MICROWAVE MOTION DETECTION SYSTEM: The microwave motion detection system shall have a transmitter designed to radiate radio frequency energy, and a receiver designed to sense Doppler shift in the frequency of the transmitted signal. The combination of transmitting unit and receiving unit shall provide a sensitive detection field, so that the movement of a human being within the protected space will generate an alarm signal. The sensitive field shall fill the protected space from wall to wall, and shall be of such nature that they will not penetrate walls, floors, or ceilings of the area protected.

2.2.6.6.1 MICROWAVE CONTROL UNIT: The microwave control unit shall provide the access/secure functions for the system. The control unit may also house the power supply.

2.2.6.6.2 MICROWAVE SENSORS: The type of emission, and maximum power output, shall be in conformance with any applicable rules and regulations of the Federal Communications Commission. Sensors shall not emit any radiation which interferes with operation of, or is hazardous to other Government

cases, the radiation shall be the minimum level that will provide stable operation, and adequate sensitivity.

2.3 MONITORING FACILITIES: The monitoring facilities shall contain all equipment necessary for reliable and efficient operation. It shall consist of some or all of the following equipment:

2.3.1 MONITOR PANELS: Monitor panels shall be of the modular, unitized, plug in type. Each monitor panel shall provide:

2.3.1.1 VISUAL INDICATORS: Three separate and independent visual indicators shall be provided.

2.3.1.1.1 LABELING: Each visual signal lamp shall be clearly and permanently marked to indicate its function.

2.3.1.1.2 COLORS:

2.3.1.1.2.1 RED shall indicate intrusion alarms registered on monitor panel. Red signals shall be labeled "ALARM."

2.3.1.1.2.2 YELLOW shall indicate that the circuit is conditioned for authorized entry. Yellow signals shall be labeled "ACCESS."

2.3.1.1.2.3 GREEN shall indicate that the circuit is conditioned for "SECURE" operation. Green signals shall be labeled "SECURE."

2.3.1.1.3 ARRANGEMENT: Where visual signal devices are augmented by manually operated keys, buttons, switches, jacks, or plugs, these devices shall be installed in or adjacent to the visual signalling device and shall be clearly marked to indicate their respective functions.

2.3.1.1.4 . SIGNAL LAMPS: Signal lamps used for visual signals shall be so connected in the circuit that a burned-out lamp, will not result in an improper or indeterminate alarm signal. Signal lamps shall be in duplicate. Lamps shall be energized from the emergency battery power supply, shall be properly rated for the operating voltage, and shall be protected with current limiting devices. To the extent practicable, all lamps shall be standardized for multiple applications in order to reduce the number of types, sizes and sockets in the system. Lamps of varying types, voltage and wattage shall have bases and sockets that will preclude incorrect replacement. Lamps shall be of long-life types having an average life expectancy of not less than 50,000 hours, and shall be operated at not more than 100 percent of manufacturers rated voltage. Signals shall be visible in daylight at distance of 10 feet.

2.3.1.2 AUDIBLE SIGNALLING DEVICES: An audible signalling device shall be provided for each monitor panel. In lieu of individual audible signalling devices, a universal audible device may be provided for the entire monitor cabinet exclusive of the power supply monitor panel. The signal devices shall be audible at least 25 feet and shall be energized from a dependable power source. If one universal audible signal device is provided for all alarm circuits, it shall be operated by a common relay, operated by signals from each monitor panel. Each monitor panel shall be provided with a silencing switch so connected that the signal can be silenced by the operator with-

out interference with audible annunciation for any subsequent alarm condition on other circuits. If separate audible alarms are provided on each individual monitor panel, they shall be similar in tone. Silencing switches shall be of the positive-reset type, i.e., when the monitor panel is reset, the audible signal shall automatically sound until silencing switch is returned to its original position.

2.3.1.3 ACCESS/SECURE FUNCTION: An access/secure function providing an indication shall be provided. The positioning of the switch at the area control unit to authorized entry (ACCESS) shall energize a RED light and audible alarm at the annunciator panel. When the switch at the monitor panel is placed in a corresponding position to the area control switch, a YELLOW light shall be energized and the RED light shall be extinguished when the circuit is reset. This will indicate that the particular circuit is in balance and operational. Transfer of the circuit from the authorized-entry mode to the fully protected mode (SECURE) shall also initiate a RED alarm signal, the YELLOW light shall be extinguished and a GREEN light shall be energized when the circuit is reset.

2.3.1.4 RESET FUNCTION: A reset function which returns the monitor panel to its normal state shall be provided. Reset switches or buttons on monitor panels shall be so designed that receipt of an alarm cannot be prevented by holding or taping down the button or switch. There shall be no mechanical linkage between the reset button and the relay or other device which

Monitor panels with Class A Line Supervision shall resist compromise by simple or complex impedance substitution, signal substitution, recording and playback techniques or random substitution of terminations. (Only systems which have been tested and approved by the Department of the Army shall be allowed in this category.)

2.3.1.7.2 CLASS "B" SUPERVISION: Class B or standard line supervisory systems shall provide good resistance to compromise of the alarm transmission lines. This class of line supervision shall indicate an alarm if electrical signals on the transmission line vary:

2.3.1.7.2.1 More than five percent in normal line signal if it consists of direct current from 0.5 milliamperes through 30 milliamperes or,

2.3.1.7.2.2 More than ten percent in normal line signal if it consists of direct current from 10 microamperes to 0.5 milliamperes: or,

2.3.1.7.2.3 More than five percent of any component of the normal line signal if it consists of an alternating current of a frequency from one through 100 cycles per second and 0.5 milliamperes through 30 milliamperes: or,

2.3.1.7.2.4 More than fifteen percent of any component of the normal line signal if it consists of an alternating current of a frequency of higher than 100 cycles per second superimposed on a direct current having any value from 0.5 milliamperes through 30 milliamperes.

2.3.1.7.3 CLASS C SUPERVISION: Class C or low line supervisory systems shall provide low resistance to compromise of the alarm transmission lines. This class of line supervision shall indicate an alarm if the line current is interrupted.

2.3.1.8 ALARM TRANSMISSION LINES: The monitor panels shall operate on closed metallic loop circuits. Systems which utilize a single conductor between the monitor panel and the protected area, or a single conductor for wiring within the protected area, or which depends upon local ground connections, neutral conductors of the electrical distribution system, non-metallic semi-conductors, metallic raceways continuity or other discontinuous conductors such as water pipes, fence material, and similar items will not be accepted.

2.3.1.9 INTERCHANGABILITY: Monitor panels shall be physically and electrically compatible so different classes of panels may be intermixed in a monitor cabinet as required.

2.3.1.10 FRONT PANEL COMPONENTS: All components on the front panel shall be mounted in such a manner that they may not be removed without first removing the front panel.

2.3.2 EMERGENCY POWER INDICATORS: Emergency power indicator panels shall be of the modular, unitized, plug in type. Each panel shall provide:

2.3.2.1 VISUAL INDICATORS: Two separate and independent visual indicators shall be provided.

2.3.2.1.1 LABELING: Each visual signal lamp shall be clearly and permanently marked to indicate its function.

2.3.2.1.2 COLORS:

2.3.2.1.2.1 AMBER shall indicate when a detector is operating on standby battery power and shall be labeled "EMERGENCY."

2.3.2.1.2.2 GREEN shall indicate when a detector is operating normally on AC power and shall be labeled "NORMAL."

2.3.2.1.3 ARRANGEMENT: Where visual signal indicators are augmented by manually operated keys, buttons, switches, jacks, or plugs, these devices shall be installed in or adjacent to the visual signalling device and shall be clearly marked to indicate their respective functions.

2.3.2.1.4 SIGNAL LAMPS: Signal lamps used for visual signals shall be so connected in the circuit that a burned-out lamp, will not result in an improper or indeterminate alarm signal. Signal lamps shall be in duplicate. Lamps shall be energized from the emergency battery power supply, shall be properly rated for the operating voltage, and shall be protected with current limiting devices. To the extent practicable, all lamps shall be standardized for multiple applications in order to reduce the number of types, sizes and sockets in the system. Lamps of varying types, voltage and wattage shall have bases and sockets that will preclude incorrect replacement. Lamps shall be of long-life types having an average life expectancy of not less than 50,000 hours, and shall be operated at not more than 100 percent of manufacturers rated voltage. Signals shall be visible in daylight at a distance of 10 feet.

2.3.2.2 AUDIBLE SIGNALLING DEVICES: An audible signalling device shall be provided for each emergency power indicator panel. In lieu of individual audible signalling devices, a universal audible device may be provided for the entire monitor cabinet exclusive of the power supply monitor panel. The signal devices shall be audible at least 25 feet and shall be energized from a dependable power source. If one universal audible signal device is provided for all alarm circuits, it shall be operated by a common relay, operated by signals from each monitor panel. Each monitor panel shall be provided with a silencing switch so connected that the signal can be silenced by the operator without interference with audible annunciation for any subsequent alarm condition on other circuits. If separate audible alarms are provided on each individual panel, they shall be similar in tone. Silencing switches shall be of the positive-reset type, i.e., when the monitor panel is reset, the audible signal shall automatically sound until the silencing switch is returned to its normal position.

2.3.2.3 ALARM FUNCTION: An alarm circuit which activates the audible and visual indicators shall be provided. A response to the failure of AC power at a detector control unit shall result in an audible signal and a visual AMBER signal light. The alarm shall remain until AC power is restored at the detector control unit, then the emergency power indicator panel shall automatically reset, the AMBER signal lamp shall be extinguished and the GREEN signal lamp shall light.

2.3.2.4 TEST FUNCTION: The emergency power indicator panel shall contain a switch for the purpose of testing panel operation. When the switch is operated, it shall simulate a power failure signal and the panel shall indicate an alarm.

2.3.2.5 LINE SUPERVISION: Line supervision shall be provided which shall indicate an alarm if transmission line continuity is interrupted.

2.3.2.6 ALARM TRANSMISSION LINES: The emergency power indicator panel shall operate on closed metallic loop circuits. Systems which utilize a single conductor between the monitor panel and the protected area, or a single conductor for wiring within the protected area, or which depend upon local ground connections, neutral conductors of the electrical distribution system, non-metallic semi-conductors, metallic raceways continuity or other discontinuous conductors such as water pipes, fence material, and similar items will not be accepted.

2.3.2.7 INTERCHANGABILITY: Emergency power indicator panels shall be physically and electrically compatible with monitor panels so they may be intermixed in a monitor cabinet as required.

2.3.2.8 FRONT PANEL COMPONENTS: All components on the front panel shall be mounted in such a manner that they may not be removed without first removing the front panel.

2.3.3 EVENT RECORDER: The event recorder shall record alarm signals from all active zones of the monitor cabinet. Each zone shall be recorded by: day of the year, time of the

day, and zone number. Each event shall be printed on paper tape from a self-contained replaceable roll which advances after each registration. The tape shall be fed past a window and into a closed receptacle or take-up reel. The last six registrations shall be visible through the window. Access to the printer shall be through a locked door. Operation shall be automatic with no controls required for the Console Operator during normal operation. Time control shall be by means of a counter which provides clock signals. This unit shall have a Digital 24 hour readout for local time. The event recorder shall be capable of storing and printing all alarms as they occur even though all zones alarm at the same time. The recorder shall also have the capability of storing alarm signals which are received during a paper change and printing after the paper change has been completed. The recorder shall contain a light which indicates when the paper supply is low.

2.3.3.1 CONTROLS: Controls available to the console operator shall be a pushbutton switch for paper advance, and a silence switch for the power indicator. Controls which shall be accessible only through a locked door shall be:

2.3.3.1.1 Pushbutton switches for correcting date and time circuits.

2.3.3.1.2 A pushbutton switch for clearing and resetting the memory.

2.3.3.2 POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2.1.13., n., of this specification.

2.3.3.3 EMERGENCY POWER INDICATOR: An emergency power indicator shall be provided which shall comply with the requirements of paragraph 2.1.13 of this specification.

2.3.3.4 MOUNTING: The event recorder shall fit into the monitor cabinet without requiring modification of either.

2.3.3.5 SYSTEM CAPACITY: The event recorder shall have the capability of being expanded to record a maximum of 999 zones.

2.3.3.6 OPTION: An option shall be available which extends the capabilities of the event recorder so that in addition to the standard requirements, it shall indicate the following modes of the system:

2.3.3.6.1 Alarm in ACCESS mode.

2.3.3.6.2 Alarm in SECURE mode.

2.3.3.6.3 Reset in ACCESS mode.

2.3.3.6.4 Reset in SECURE mode.

2.3.3.6.5 Paper advance.

2.3.3.6.6 Memory reset.

2.3.4 SECURITY COMMUNICATIONS SYSTEMS: The Security Communication system shall provide a link between the monitor cabinet and selected remote locations. The communication control unit to be located in the monitor cabinet shall contain all necessary relays, coils, ringing circuits and power supplies to operate the system. The communication control unit shall consist of a panel which shall be mounted adjacent to the zone to which it applies. The panel shall contain a light and a switch for each

telephone position. The system shall have the ability to place incoming calls on "HOLD." A telephone handset shall be provided, mounted on the monitor cabinet.

2.3.4.1 OPERATION: An example of the system operation is as follows: If telephone No. 3 is picked up at its remote position to call into the guard office, the light and audible signal for position No. 3 on the monitor console shall actuate. When the switch is thrown to "ON" at position No. 3, connecting the telephone instrument on the monitor console to circuit 3, the buzzer will go off. When the position 3 remote telephone is hung up, an audible signal will actuate until the switch is thrown to the "OFF" position, disconnecting the circuit and turning the light and audible indicator off. If the console operator desires to call a remote position, the switch for that position is thrown to "ON" and the bell on the telephone at the remote position shall ring until the handset is picked up.

2.3.4.2 POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2.1.13 of this specification.

2.3.5 MONITOR CABINET: The monitor cabinet shall be capable of housing monitor panels, emergency power indicators, event recorders, security telephone systems, power supplies, and any other equipment necessary for the proper operation of the system. The monitor cabinet shall conform to the following:

2.3.5.1 LAYOUT AND ARRANGEMENT: The monitor cabinet shall be of the open front type which shall be an attractive,

durable, logically arranged unit. All visual signals and components requiring manual manipulation by the console operator shall be accessible from the front. All other components shall be mounted inside of the enclosure, and shall be readily accessible for maintenance through doors with hinges and locks. Maintenance adjustments of equipment shall be secured against change of their sensitivity by the operator or other unauthorized personnel. All equipment mounted in the monitor cabinet shall be mounted in such a manner that the mounting hardware for the equipment is concealed behind locked doors or, in lieu of such mounting, shall be provided with individual tamper switches connected so as to sound the tamper alarm if any piece of equipment is removed.

2.3.5.2. ENCLOSURE: The enclosure shall comply with the requirements of paragraph 2.1.12. of this specification.

2.3.5.3. POWER SUPPLY: The power supply shall comply with the requirements of paragraph 2.1.13 of this specification.

2.3.5.4. EMERGENCY POWER INDICATOR: The emergency power indicator shall comply with paragraph 2.1.13 of this specification.

2.3.5.5. REMOTE SIGNALLING: The monitor cabinet shall have the capability of providing signals which may be used for remotely supervising the console operation. The system shall be capable of any of the following modes of operation:

2.3.5.5.1. A single remote signal if any of the zones in the cabinet alarm.

2.3.5.5.2. A single remote signal if one of the zones in the cabinet alarm.

2.3.5.5.3. A single remote signal if a preselected group of zones in the cabinet alarm.

SECTION V

STANDARDS FOR INSTALLATION OF INTERIOR INTRUSION DETECTION SYSTEMS

A. INSTALLATION REQUIREMENTS: Installation of Interior Intrusion Detection Systems shall be neat, efficiently planned, and shall provide the level of performance required by the technical section of this specification. In addition, the installation shall be as listed below:

1. CABLING: All cables installed as part of the Interior Intrusion Detection System shall comply with the following:

a. POWER CONDUCTORS: Power conductors for supplying 120 volt AC power to the system shall be of solid copper not smaller than No. 12 AWG, with moisture-resistant rubber insulation type RW or RH-RW conforming to Federal Specification No. J-C-103, or moisture-resistant thermoplastic insulation type THW conforming to Federal Specification No. J-C-129 as applicable.

b. LOW VOLTAGE CONDUCTORS: Low voltage conductors shall be of solid soft drawn copper, with moisture-resistant rubber insulation type RF-2, or thermoplastic insulation, type TF having a nominal thickness of not less than 1/32 inch and conforming to NBFU No. 70. Wire connectors of insulating material, or solderless pressure connectors in conformance with Federal Specification No. W-S-610 shall be used for all connections and properly taped. Conductors shall be not smaller than No. 22 AWG.

2. CONDUIT: Conduit shall be installed in accordance with Article 346 of the National Electrical Code. Minimum size of conduit shall be 1/2 inch. No threadless fittings or couplings

shall be used in the system. Conduits shall be supported and secured at intervals of not more than 8 feet. Exposed conduits shall have runs installed parallel or perpendicular to walls, structural members, or inter-sections of vertical planes and ceilings. Field-made bends and offsets shall be made with an approved Hickey or conduit-bending machine. Changes in direction of runs shall be made with symmetrical bends or cast-metal fittings. Where conduits connect to sheet steel enclosures of monitor cabinet, power supplies, and other similar enclosures, they shall be fastened with two locknuts where insulating bushing are acceptable. Bushings shall be installed on ends of all conduits and shall be of the insulating type. Crushed or deformed conduits shall not be installed. Trapped conduits in damp and wet locations shall be avoided where possible. If trapped conduits are unavoidable, the ends shall be plugged with an approved R. T. V. sealing compound after wires are pulled therein. Care shall be taken to prevent the lodgement of plaster, dirt, or trash in conduits, boxes, fittings, and equipment during the course of construction. Conduits shall be entirely free of obstructions, or shall be replaced. Conduits crossing expansion fittings shall be of suitable material to compensate for building expansion and contraction. Conduits installed underground, or under slabs on grades shall be factory coated with coal-tar enamel or plastic. Field applied coatings shall be with pressure sensitive plastic tape. Wooden plugs inserted in concrete or masonry are not acceptable as a base for conduit fastenings,

nor shall conduits or pipe straps be welded to steel structures. Conduits shall be secured by pipe straps or supported by wall brackets, strap hangers, or ceilings trapeze, fastened by wood screws on wood, toggle bolts on hollow masonry units, expansion bolts on concrete or brick, machine screws on steel work, nailtype nylon anchors or threaded studs driven in by a power charge and provided with lock washers and nuts, are acceptable in lieu of expansion bolts, or machine or wood screws. Power-driven studs or expansion anchors and bolts will not be permitted closer than 12 inches to prestressed steel in prestressed concrete work. Nails shall not be used as a means of fastening conduits. Conduit outlet boxes, pull boxes, junction boxes, conduit fittings and similar enclosures shall be cast metal or malleable metals conforming to Federal Specification No. W-C-586, with threaded hubs or bodies. Where specifically authorized by the Contracting Officer, electric metalling tubing, armored cable, nonmetallic sheathed cable, or flexible conduit is permitted. Pull and junction boxes shall be provided with tamper switches which shall conform with the requirements of Section VI, paragraph 2.2.12.2. In lieu thereof, the covers shall be tack welded or held in place with twist-off, or one-way machine screws which cannot be readily removed without cutting or drilling. Cables shall not be spliced or terminated in pull or junction boxes.

3. CABLE TERMINAL BOXES: Cable terminal boxes shall be used for the splicing or termination of cables. The enclosure shall

conform to Section IV 2.1.12.

4. GROUNDING: Neutral conductors, conduits, junction boxes, cabinets, cable messengers, and all non-current carrying metallic parts of equipment shall be ground in accordance with NBFU No. 70.

5. REPAIR OF EXISTING WORK: The work shall be carefully laid out in advance. Where cutting, channeling, chasing, or drilling of floors, walls, partitions, ceilings, or paving, of other surfaces is necessary for the proper installation, change of location, support, or anchorage of equipment, etc., this work shall be done, and any damage to the building, paving, piping, or equipment shall be repaired and refinished by skilled mechanics of the trades involved at no additional cost to the Government. Conduit and fittings run exposed on finished walls and ceilings shall be painted with two coats of paint to match the surface on which they are mounted.

6. ACCEPTANCE TESTS: Upon completion of installation of the system, tests shall be conducted by the contractor during a continuous period of 48 hours to determine system conformance to requirements of this specification. Tests shall be conducted in the presence of the contracting officer or his authorized representative who may suspend or discontinue the tests at any time performance is considered unsatisfactory. Resumption of testing will cover the previously untested elements, and any completed elements at the discretion of the contracting officer who will make written notations of the time, cause and other conditions prevailing at the time each alarm signal is received.

The contractor shall furnish all test personnel except for those required to maintain alarm records for the contracting officer. Test instruments and equipment of the accuracy necessary to perform the test shall be furnished by the contractor.

B. DOCUMENTATION AND TRAINING: The installation of the Interior Intrusion Detection System shall include the furnishing of documentation providing information on the system as installed and a training program for operating personnel.

1. TRAINING OF OPERATING PERSONNEL: The contractor shall conduct a training program of designated operating personnel. The training program shall include instruction on the operation of the monitor facilities, equipment in the secured areas, and procedures to be followed in requesting emergency service. Training shall be presented by a qualified instructor using such drawings, charts, diagrams, training aids, and demonstrations with such components as are deemed necessary by the contracting officer to a comprehensive training program.

2. OPERATION AND MAINTENANCE MANUAL: The contractor shall furnish three copies of a manual containing complete operating and maintenance instructions for the Interior Intrusion Detection System. This manual shall be prepared in a manner and form to provide technical data required by trained personnel to operate, test and maintain the system. Drawings, schematics, tables, charts, and photographs shall be included. A draft of the manual shall be submitted for the contracting officer's approval as to adequacy, prior to preparing in final form. The manual shall incorporate the following in the order indicated:-----

a. COVERS: Front and back covers shall be of durable stock with the following printed on the front cover:

- (1) Title with correct nomenclature;
- (2) Contract number;
- (3) Date of publication;
- (4) Proprietary notice to read "Prepared under contract No. by (Name of Contractor, For (Name of Department or Agency));

(4) Classification of manual (if any) plainly and conspicuously marked at the top and bottom of the page in accordance with the Industrial Security Manual.

b. TITLE PAGE: The title page shall be the same information which appears on the front cover.

c. TABLE OF CONTENTS: The table of contents shall list all important subdivisions of the manual.

d. GENERAL: The general section shall contain an overall description of the system including types of equipment installed, arrangement of the system, etc.

e. TECHNICAL SECTION: The technical section shall contain detailed information on the equipment included in the Interior Intrusion Detection System. It shall include:

- (1) General,
- (2) Theory of operation,
- (3) Installation,
- (4) Maintenance and adjustment,
- (5) Troubleshooting,

f. OPERATION SECTION: The operation section shall contain recommended procedures for operating the system.

3. AS-INSTALLED DRAWINGS: Upon completion of the work, the contractor shall neatly modify the approved shop drawings to show details of the system as actually installed. Three prints of such drawings shall be furnished to the facility security officer, and one set of prints shall be furnished for the contracting officer.

C. GUARANTEE: The Interior Intrusion Detection System installed under this specification shall be guaranteed for a period of one year from the date of acceptance thereof, either for beneficial use or final acceptance whichever is earlier, against defective materials, design, and workmanship. Upon receipt of notice from the Government of failure of any part of the guaranteed system during the guarantee period, new replacement parts shall be furnished and installed promptly by the contractor at no additional cost to the Government.

SECTION VI
STANDARDS FOR
PREVENTION MAINTENANCE AND EMERGENCY SERVICE

A. GENERAL:

In some instances it may be necessary for using activities to contract with commercial alarm companies for maintenance and emergency service in order to insure continuous operation of the system.

The following paragraphs establish standards for all maintenance and emergency service:

1. Preventive Maintenance:

a. Not less than once each month the alarm system shall be inspected and tested by trained technicians. Each operating unit shall be tried to assure an alarm will sound upon violation of the alarm system. All batteries will be tested under load to determine the expected useful life remaining in cells. Any necessary recharging or replacing of batteries shall be accomplished immediately.

b. If adjustments are necessary to the equipment, they shall be performed at this time. If such adjustments affect the sensitivity of the alarm system, this shall be reported to the security officer in charge of the area.

c. Should any test reveal a weakness in the degree of security provided by the system, or should any evidence be found of tampering with the equipment or connecting lines, switches, antennas, microphones, transducers, grids foil or other sensitive elements; also, that any adjustment

has been changed, or that any equipment or sensitive element has been moved or removed, this shall be immediately called to the attention of the security officer in charge of the area.

d. Upon completion of each monthly inspection, the security officer, or his designated representative, shall be asked to sign the contractor's inspection form. This form shall carry notations of the voltage readings of all batteries, replaced parts, adjustments and evidence of any tampering.

e. The contractor shall replace any component parts of the alarm system that have failed due to normal usage during the term of this contract and any extension thereof.

f. The hours of work of monthly inspections, or testing in any Government premises shall be performed between the hours of 8 o'clock A.M. and 5 o'clock P.M. exclusive of Saturdays and Sunday.

2. EMERGENCY SERVICE:

a. The contractor shall agree to provide emergency service 24 hours a day, seven days a week, Saturdays, Sundays, and Government holidays inclusive upon receipt of oral or written notification of equipment failure, or improper functioning of any alarm system component. The contractor shall cause necessary qualified service technician to respond to this emergency request within ninety minutes after receipt of such notification. Notification to the contractor shall be by authorized person(s) designated by the contracting officer.

b. Every effort shall be made to restore the system to normal operation in the shortest possible time. The duty officer or other responsible person shall be notified by the contractor of the estimated time required to service, adjust, and restore normal operation of the alarm system after an initial inspection has been made by the service technician.

c. An emergency service report shall be prepared by the contractor for the proponent agency. This report shall indicate the nature of the service call, response time, correction applied, and amount of time required to restore system.

3. SERVICE LIMITATIONS:

a. The contractor shall be obligated under the contract to service only Government equipment included as part of the system or systems.

b. The contractor shall not be responsible to repair damage to the alarm caused by the following:

(1) Damage to any equipment connected to the electric power supply caused by a change in the value or characteristics of the electric power supplied.

(2) Damage to any equipment connected to leased or Government owned telephone lines, or connecting cables, caused by the application of any electric source to these lines or cables that affects the alarm system, such as:

(a) Lightning.

(b) Telephone line or cable failure.

(c) Testing by personnel other than the contractor's employees, unless under the contractor's observance.

(d) Connecting other service on the same telephone pair or cable.

(c) Other service on the same cable of such a nature as to cause damaging induced current to the alarm equipment.

(3) Damage from misuse: The contractor shall furnish operating instruction and give additional information during normal working hours, as furnished by the manufacturer.

(4) Damage from missiles, falling objects, fire, theft, explosion, earthquake, windstorm, hail, water, flood, vandalism, riot, civil disturbance, or acts of war.

c. The following conditions that may require service or liability against the contractor are hereby excluded from this contract.

(1) Any modification, extensions, deletions, or other changes in the alarm system require due to changes of space, design or operation in the secured area are not covered by this contract.

(2) Any interruption to the alarm protection by workmen in the area, other than the contractor's employees are not covered by this contract.

(3) The contractor does not assume any property damage liability or personal injury liability due to the operation of a Government-owned and operated alarm system.

4. Evaluating contractor proposal for maintenance and emergency service.

a. In evaluating the ability of a contractor to perform preventive maintenance and emergency service, several factors should be considered, they are:

(1) Response: The procedures established by the contractor for responding to emergency service calls. For an example: Whether they use a telephone answering service to receive the calls or a part of their 24 hour service organization and whether the responding technicians are full time

qualified personnel, or are working on a part time basis in the evenings.

(2) Training: The training program for service technicians is very important. Consideration should be given to the type of program in effect and whether this program is of a general nature or specifically oriented to the equipment which will be installed in the installation.

(3) Spare Parts: The contractor should maintain an adequate supply of spare parts so that a system failure may be repaired by direct replacement of parts, rather than taking the defective components back to the shop and repairing them. Quantities should be such that at least ten simultaneous failures to a particular type of equipment can be easily handled.

(4) Previous record of performance. If not locally available an inquiry should be made to the OPLS, DA, ATTN: PMCS-S.

SECTION VII .

PROCUREMENT OF INTRUSION DETECTION SYSTEMS:

1. GENERAL:

Based upon the guidance set forth in the preceding sections a decision should have now been made regarding the precise intrusion detection equipment needed to accomplish the degree of physical security required. Having accomplished this, the next step is to assemble the necessary data into what we shall term the "Intrusion Detection System Requirements". This package must describe in exact terms to all interested commercial bidders, what is required to satisfy the contract for the total system procurement as concerns equipment components, equipment standards, installation and service requirements plus warranties and guarantees expected. (Any inadvertent omissions from this package will ultimately raise the system "contract price" through requirements for subsequent contract "Add Ons.")

The completed package along with "fund citations" to cover costs is then forwarded to the local DA purchasing office. (Definitive requirements for accomplishing this step can be locally obtained.)

2. REQUIREMENT PACKAGE: Prior to the preparation of the procurement package, necessary consideration should have been given to the environmental and construction characteristics of the area requiring protection, the operational requirements of the area, the classification or value of material being protected in the area, and any regulatory standards which the area must meet. After careful evaluation you have now decided upon the system required. After determining the intrusion detection equipment requirements, for an area, a procurement package is prepared and will include as a minimum the following:

a. A system description which outlines in detail the following: (See Appendix B)

(1) The functional description of the Intrusion Detection System requirements.

(2) The type of cabling to be used in the system.

(3) Installed performance requirements for each component of the system. (Standards will be as stated in Section IV).

(4) Items which will be government furnished or contractor furnished.

(5) Description of the arrangement and layout of the monitoring facilities.

(6) Operating time requirement for emergency power.

(7) Remote test requirements.

(8) Specific conduit requirements.

(9) Description of existing alarm systems (only applicable when solicitation is for tie-in with existing equipment).

(10) Description of utilities provided at the job site by the Government.

b. A zoning chart (See Appendix B) should be included in the procurement package outlining the number of zones required in numerical order, type of protection required in each zone, class of monitor panel line supervision required, location of zones by building and room number.

c. Drawings showing the location of the individual zones within the building and desired location of control units within each zone. (See Appendix B). Where more than one building is included in the system, a site layout defining distances and signal line routing will be included. The drawings shall include a description of the physical construction of the area, i.e., poured concrete, cinder block, dry wall, etc.

d. A statement which requires that each interested commercial bid proposal will contain the following:

(1) MATERIALS AND EQUIPMENT LIST: The prospective contractor shall submit to the contracting officer, a complete schedule of materials, devices and equipment which the contractor proposes to incorporate in the work. This list shall include catalog numbers, diagrams, drawings, reports, and other descriptive data. Any materials, components, and equipments which are not in accordance with the specification requirements will be rejected.

(2) DRAWINGS: The prospective contractor shall submit copies of all drawings which pertain to the installation of the system to the contracting officer for review and approval. As a minimum they shall contain:

(a) MONITOR CABINET: Details of the monitor cabinet(s) including: layout of cabinet(s), arrangement of monitor panels, emergency power panels, telephone equipment, and any other equipment included in the system.

(b) POWER SUPPLY: Details of the computations used for determining ampere-hour capacity of standby batteries to meet specification requirements for operation of the system on emergency power.

(c) MOUNTING BRACKETS: Details of mounting bracket for magnetic switches and other detectors.

(d) CAPACITANCE GRIDS: Details of standard capacitance grids and/or grills.

(e) WIRING DIAGRAM: Complete system wiring diagram identifying all wire facilities associated with the system, each system component in its relative location; also the number, size, identification, and types of conductors required for interconnection between system components.

(f) GUARD OFFICE LAYOUT: A drawing shall be furnished which shows the layout of the monitor cabinet and other equipment in the guard office.

(g) LAYOUT OF SECURED AREAS: A drawing shall be furnished for each area to be protected showing in detail the location and types of detectors and control units as they are to be installed.

3. EVALUATION OF PROPOSALS:

a. When the proposals are received from the various bidders, the technical portion of such proposal should be evaluated by the contracting officer and the using agency. Proposals should be first divided into two categories: (1) Proposals which meet the minimum standards set forth in the procurement package, and therefore, are responsive to the solicitation, (2) proposals which do not meet the minimum requirements for the procurement package, and therefore, are not responsive to the solicitation.

b. Detailed evaluation should then be given to each proposal which is considered to be responsive to the solicitation, and the proposals should be graded technically from the most desirable proposal down to the least desirable. When this is done, a comparison can be made between the price offered by the various bidders, the quality of the system being proposed and then the selection of the contractor that offers the best value to the government at the lowest cost.

contractor completely understand the specification and in fact whether he can furnish the precise equipment required in the bid package. In some instances, this may not be completely determined until the final inspection of the installed system.

(3) Since the IIB method of procurement allows only an after the fact check for determining whether a contractor understood the total requirements of the bid package, this alternate should be carefully considered before being used.

b. Request for proposal (RFP):

(1) The primary difference between the IIB and RFP is that the RFP requires interested contractors to submit a complete technical proposal describing the exact equipment that he will furnish under the contract, the exact arrangement of the equipment within each preferred area, the layout of the security facility, plus the price and delivery of the system along with any other requirements which the using activity may require.

(2) In this type of procurement the contracting officer, along with security and technical personnel of the using agency, should completely evaluate each commercial solicitation to determine each bidder understanding of the requirements to include the individual items of equipment (components) that the bidder proposes to supply, e.g., whether the equipment meets the specification standards and any alternative proposals that the commercial bidder may wish to submit.

(3) Under an IIB the government is not bound to award the contract to the lowest bidder and therefore the award selection can be made to the proposal which offers the best value to the government e.g., which solicitation in fact provides the best quality system for the lowest cost.

4. EVALUATION OF PROPOSALS:

a. When the proposals are received from the various bidders, the technical portion of such proposal should be evaluated by the contracting officer and the using agency. Proposals should be first divided into two categories: (1) proposals which meet the minimum standards set forth in the procurement package, and therefore, are responsive to the solicitation, (2) proposals which do not meet the minimum requirements of the procurement package, and therefore, are not responsive to the solicitation.

b. Detailed evaluation should then be given to each proposal which is considered to be responsive to the solicitation, and the proposals should be graded technically from the most desirable proposal down to the least desirable. When this is done, a comparison can be made between the price offered by the various bidders, the quality of the system being proposed and then the selection of the contractor that offers the best value to the government, can be made.

SECTION VIII

A. QUALIFIED INTRUSION DETECTION EQUIPMENT

1. General

a. The purpose of this supplement is to provide Army field elements with an interim listing of those commercial manufactured intrusion detection (ID) equipment for indoor application which have been previously used by DA/DOD field elements and which are considered acceptable until such time as a DA qualified products listing is published. Inclusion of equipment on the DA QPL will be as the result of DA laboratory tests. Data contained in this supplement will not be released in any context that may indicate that equipment/companies not listed would not be acceptable or approved if tested.

b. This supplement is not a complete catalog or current acceptable security detection equipment. Other firms or manufacturers may have equally acceptable devices; however, until such products are subject to test, and a favorable evaluation is concluded by a DOD/DA testing facility, its use cannot be recommended at this time. Companies submitting bids on open DA negotiated contracts for ID systems, and whose proposed equipment is not listed herein, must be subjected to test and evaluation. Assistance in determining whether a product meets the standards of the DA Intrusion Detection Equipment Specification may be obtained from the following two facilities.

(1) Intrusion and Barrier Laboratory, MZRDC, Fort Belvoir, Virginia.

(2) Intelligence Materiel Development Office, Fort Holabird, Maryland.

(Qualifying tests will require delay in the procurement, therefore, additional time factors of up to four months can be expected. An information

copy of requests for testing of specific devices will be forwarded by the requesting activity to the Office of The Provost Marshal General, DA, ATTN: PMGS-S.)

2. Alarm components and system data.

a. This list will be expanded as other products are determined to be acceptable. The components and data listed below have been compiled on the basis of actual field use. Where no specific items are listed, products being considered in these groupings must be cleared through Office of The Provost Marshal General, Department of the Army.

(1) Detectors

(a) Electromechanical Devices

(1) Access/Secure Control Unit

(a) Wells Fargo - Model CU-3

(b) Mosler - Model DNS.4

(2) Simple Magnetic Switch

(a) Wells Fargo SM-2, SM-5

(3) Balanced Magnetic Switch

(a) ADT 4035, 4036

(b) Johnson Service MDS - 100 with housing

(c) Kiddie DR-845 with housing

(d) Mosler MS-5 WT

(e) Wells Fargo SM-1, 3, 4

(4) Foil

- (5) Protective Wiring
- (a) Underwriters Laboratory listed - no model numbers
- (6) Holdup Devices
- (a) Pushbutton - WF HU-1
 - (b) Footrail - WF HU-2
- (7) Heat Detectors
- (a) ADT C-909
 - (b) Honeywell T-487A, T-487B
 - (c) Mosler VT-3
 - (d) Wells Fargo HD-1
 - (e) Photo Electric System (None tested) - WF PE-1
- (8) Vibration Detection
- (a) ADT 7122, 7122, 7128
 - (b) Honeywell TC 10A w/w/ - 676 C Panel
 - (c) Mosler Stentinel V
 - (d) Wells Fargo CU-2 w/ DV-1
- (9) Audio-Detection System - None tested
- (10) Capacitance System
- (a) ADT 7304
 - (b) Honeywell W837A
 - (c) Mosler AL-26PSLT
 - (d) Wells Fargo CU-1
- (11) Motion Detection System
- (a) Sonic and Ultrasonic
- (1) ADT 7127-003
 - (2) Kiddie HC-140

- (3) Mosler MC-140
- (4) Wells Fargo CU-4
- (5) Honeywell W711A w/TC-7000 C and Disconnect device
- (6) Sonaguard - Portable Alarm - Model #628E

(b) Microwave

- (1) Johnson Service G-7, G1-1
- (2) Advanced Devices 210
- (3) Wells Fargo CU-5

(c) Monitor Facilities

(1) Monitor Panels

(a) High Security (Class A)

- (1) ADT 7111, 7124
- (2) Mosler AL-31
- (3) Wells Fargo MP-1

(b) Medium (Standard) Security (Class B)

- (1) ADT 5930
- (2) Honeywell W657
- (3) Johnson Service BG 1006
- (4) Mosler AL-38
- (5) Wells Fargo MP-2

(c) Low Security (Class C) - WF MP-3

(d) Emergency Power Indicators

- (1) Mosler EPP
- (2) Wells Fargo MP-4

(e) Event Recorders WF ER-1

(f) Security Communication Systems - none tested

(g) Monitor Cabinets (Currently under test)

FOR OFFICIAL USE ONLY

LIST OF MANUFACTURERS

American District Telegraph (ADT)
1675 Connecticut Avenue, N.W.
Washington, D.C. 20009

Honeywell Corporation
Commercial Division
4926 Wisconsin Avenue, N.W.
Washington, D.C. 20016

Johnson Service Company
Security Sales Division
900 North Stafford Street
Arlington, Virginia 22203

Walter Kiddie Company, Inc.
Alarm Products Division
675 Main Street
Belleville, New Jersey 07109

Mosler Research Products, Inc.
Electronic Security Division
1401 Wilson Boulevard
Arlington, Virginia 22209

Wells Fargo Alarm Services
Government Division
1004 6th Street, N.W.
Washington, D.C. 20001

Sonaguard Electronic Auto Alarm
119 Dover Street
Somerville, Massachusetts

FACILITY SURVEY CHECKLIST
FOR
INTRUSION DETECTION ALARM SYSTEMS

1. Facility _____
2. Location _____
3. Unit Conducting Survey _____
4. Individual's Name (Person Preparing Inquiry) _____
 - a. Title _____
 - b. Address _____
 - c. Phone _____
5. Date of Survey Conducted _____
6. Purpose (State what you want to protect, classification of data, weapons storage, monetary or other intrinsic value. _____

7. Name and general description of outdoor areas, buildings, indoor areas and objects to be protected:
 - a. Size of outdoor area _____
 - (1) Fencing type and height _____
 - (2) Patrol roads or footpaths (type) _____
 - (3) Security lighting (type and intensity) _____
 - (4) Describe terrain _____

 - (5) Environmental extremes (Temperatures and climate, adjacent activities) _____
 - b. Types of Buildings (description) _____

(1) Numbers of doors (list each type and use, i.e., personnel, vehicle, overhead, emergency exit, etc; also any special construction such as dutch, glass, vault, roll-up, etc.) _____

(2) Number, type and size of windows (list quantities of each size and type separately as well as structural barriers over windows) _____

(3) Number, type and size of accessible openings other than windows and doors (list all openings greater than 96 square inches in areas that have a minimum dimension in excess of six inches, include all ducts, grills, panels, vents, etc., that do not provide physical barriers equivalent to the walls, floors and ceilings in which they are located) _____

c. Indoor areas: Dimensions, shapes and utilizations of indoor areas to be provided with space or motion detection (Explain type of furnishings, height and configuration of shelving or other storage) _____

(1) Type of construction (wood, metal, masonry) _____

(2) Temperature extremes and extreme air velocities _____

d. Objects: furnish size, shape, location and composition of objects to be protected _____

8. Total number of areas or zones to be protected (number of separate circuits to be individually annunciated) _____

9. Type of system preferred: Local alarms _____ Central Station Alarms _____ Remote Annunciator _____

10. Type of guard system to be supported: Fixed post sentries _____ Foot Sentry-roving _____ Foot Sentry-Fixed Patrol _____

Sentry-Dog team _____ Motorized patrol _____ One man patrols _____ Buddy System _____ Size of Sabotage

Alert Team _____ Size of Backup alert force _____

11. Surveillance interval (in minutes): One man surveillance interval _____

Duress response interval (response time of second guard) _____

Sabotage alert team response _____ Backup alert team response _____

12. Travel Distances (Miles): Perimeter of patrolled area _____

Motorized patrol tour _____ Maximum foot tour _____, Distance

from sabotage alert station to farthest protected item (travel route) _____

_____, Distance from backup alert force station to the farthest

protected item _____ . Distance between communication points

(phones, radios or fixed sentry stations) _____ .

13. Communications available for guard use: Vehicle radio _____
Personnel radio _____ Guard Telephone Net-telephones _____ or
Phone jacks _____ Automatic Ringdown _____, Dial Station
_____. Watchman call stations _____ Tour clock stations
_____ Telephone circuits aerial _____ or underground _____

14. Electrical Power: Commercial _____ Standby Generator _____
Emergency Generator _____ Emergency Battery Power _____

a. Security Lighting _____ Perimeter _____
Area _____ Building _____

b. Electrical service to buildings _____ (list all areas,
buildings and objects to be protected where normal electrical service is not
available) _____

15. Access Controls: Will alarm system be required to provide: Intrusion
Detection only _____? Authorized access indications _____?
Positive authorized ingress _____ and egress _____ control?
Protection against system compromise by personnel authorized access to area
_____?

16. Protection Reliability: Will alarm system be required to provide auto-
matic alarm signals for the following conditions:

- a. Forced entry only? _____
- b. Unintentional improper operation or accidental damage? _____
- c. Disablement by operations personnel during authorized access? _____
- d. Complete fail-safe reliability against any/all above exposures? _____
- e. Other (explain)? _____

17. Performance tests: Will system performance be subject to tests and verification by:

- a. The systems' internal fail-safe features only? _____
- b. Guard personnel on sentry duty? _____
- c. Guard supervisory personnel monitoring the alarm system annunciation? _____

-
- d. Operational personnel authorized access to protected items? _____
 - e. Maintenance personnel responsible for the alarm system? _____

18. Alarm annunciation and supplementary signaling desired.

- a. Local audible _____ Distance in feet _____
- b. Local visual _____ Visual distance _____
- c. Central station audible and visual alarms (alarm signal only) _____
- d. Secure condition indicators _____, Local _____,
Central Station _____ Remote station _____
- e. Authorized access (open) signals _____, Local _____
Central Station _____ Remote Station _____
- f. Deactivated (unmanned) condition signals _____ (Not
available for local alarm systems) Central Station Panel _____
Remote Station Panel _____
- g. Hold-up Signals
 - (1) Manual from protected areas to central station _____
 - (2) Manual from central station to response forces _____

19. Remote annunciation requirements: Will alarm system require one or more of the following:

- a. Local alarms automatically transmitted to guard office.

b. Central station alarms automatically transmitted to remote annunciator for other alert force _____

c. Will remote alarm signals be:

(1) Common alarm (single annunciator for all alarm systems at the protected area) _____

(2) Area alarm (one annunciator for each group of buildings or several circuits in one building) _____

(3) Zone alarm (individual remote annunciators for each zone or circuit at each protected premises) _____

20. Furnish any special considerations not covered by the foregoing questions:

PROCUREMENT PACKAGE OUTLINE

SYSTEM DESCRIPTION

1. Functional description of Intrusion Detection System requirements:

(Explain general requirements of the system desired to include preparation of a zone chart establishing the precise number of zones required with types of equipment desired per zone and a diagram showing actual location of each zone (See Incl 1 & 2).

2. Requirements of monitoring facilities:

a. Type of monitor panels (Check applicable items)

(1) Class A _____, _____ qty

(2) Class B _____, _____ qty

(3) Class C _____, _____ qty

(4) Emergency power indicator _____, _____ qty

b. Security telephone system

Required _____, _____ qty of instruments

Not required _____

c. Event recorder

(1) Standard _____.

(2) With Options _____.

d. Monitor cabinet

(1) Number of active zones _____.

(2) Number of spare zones _____.

(Combination of active and spare zones should be an even multiple of 10)

e. Description of any special requirements such as: remote panels, status maps, etc.

3. Standby Power Requirements (Check one)

12 hours _____ (Standard)

24 hours _____

36 hours _____

48 hours _____

4. Remote test

Required _____

Not required _____

5. Conduit requirements (Check appropriate items)

a. None _____

b. E.M.T. _____

c. Rigid _____

d. Location of Conduit (Check one)

(1) Entire system _____

(2) Between control unit and monitor cabinet _____

6. Description of existing intrusion detection systems (if new system is to tie-in with existing system):

7. Description of government furnished items:

a. AC power: Furnished _____ . Not furnished _____ .

(1) to nearest disconnect switch _____ .

(2) to locations as specified by contractor _____ .

b. Signal lines: Furnished _____ . Not furnished _____ .

(1) Leased telephone lines _____ .

(2) Proprietary telephone lines _____ .

(3) Direct wire runs _____ .

c. Government furnished equipment (describe).

8. Types of detectors required (check applicable items).

a. Electro-Mechanical devices

(1) Access/secure Control Unit _____ .

(2) Magnetic Switch

(a) Simple _____ .

(b) Balanced _____ .

(3) Foil _____ .

(4) Protective Wiring _____ .

(5) Hold-Up Devices

(a) Push button _____ .

(b) Foot rail _____ .

(6) Heat Detector _____ .

b. Photo-Electric system _____ .

c. Vibration Detection System _____ .

d. Audio Detection System _____ .

e. Capacitance Detection System _____ .

f. Motion Detection System

(1) Ultra-sonic _____ .

(2) Microwave _____ .

(3) Other _____ .

Zone Number	Location of Zone		Electro-Mechanical Systems										Capacitance System			Motion Detection System		Monitor Cabinet				Remarks																
	Building	Room	Foil	Window	Door	Wall	Window	Door	Wall	Vent	Other (Explain)	Magnetic Switch	Simple	Balanced	Heat Detector	Button	Foot Rail	Access/Secure Control	Photo Electric	Audio Detector	Vibration Detector		Door Grid	Window Grid	Duct Grid	Other (Explain)	Sonic/Ultrasonic	Micro-wave	Emergency Power Indicator	Class "A" Supervision	Class "B" Supervision	Class "C" Supervision	Remote Test	Security Telephone				
1	214	Front doors										X						X																				
2	214	Jack doors										X						X																				
3	214	Reading Deck										X						X																				
4	214	109										X						X																				
5	214	109																X																				
6	214	112										X						X																				
7	214	112																X																				
8	214	111										X						X																				

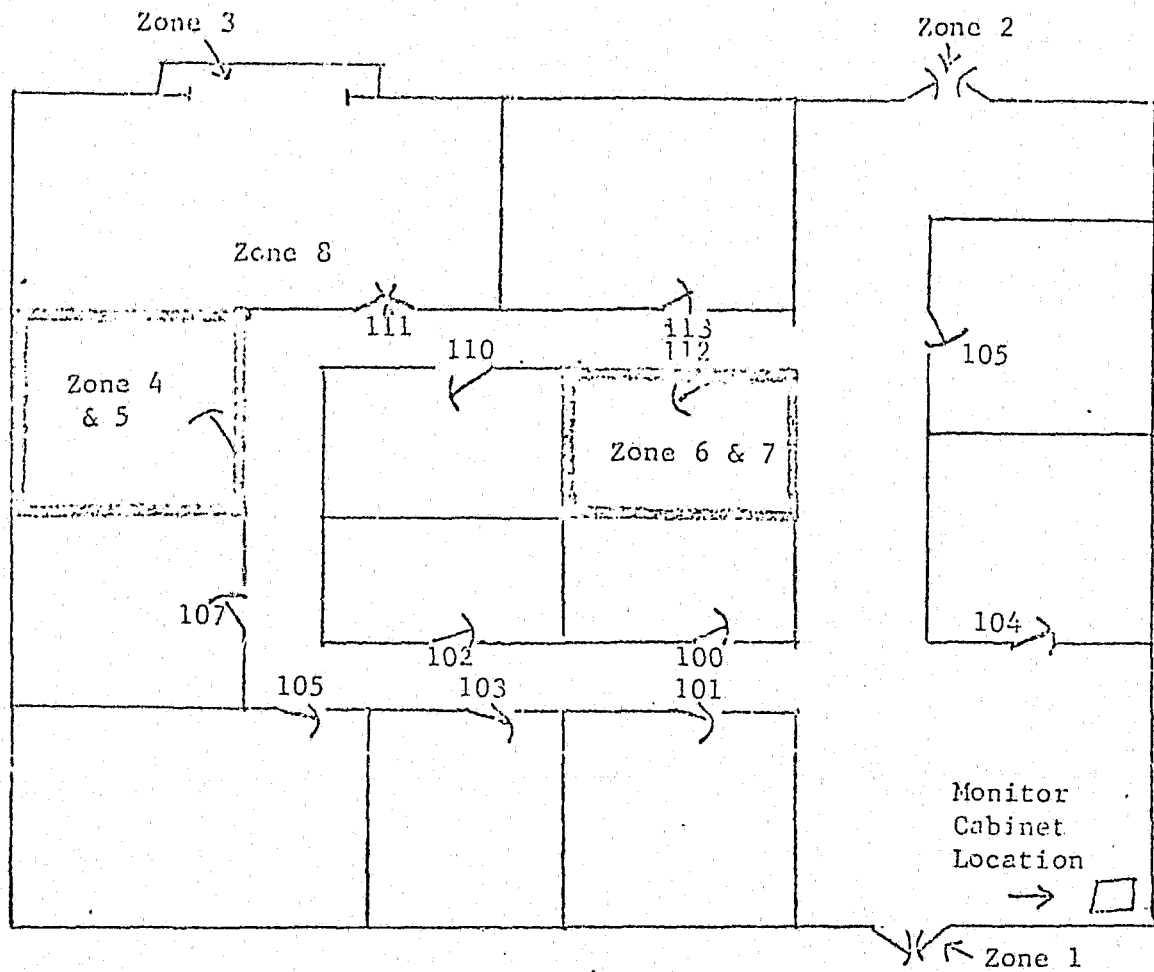
Zoning Chart for

BUILDING 214, 1st Floor

Page 1 of 1 Pages

Incl 1
Appendix B

TYPICAL DRAWING AND ZONE CHART



BUILDING 214
1st Floor

TYPICAL DRAWING

Incl 2
Appendix B

END

7 11/15/1960