DOCUMENT RESUME

00056 - [A1052008]

Vulnerabilities of Telecommunications Systems to Unauthorized Use. B-146864; LCD-77-102. March 31, 1977. Released April 26, 1977. 29 pp.

Report to Rep. Paul N. McCloskey, Jr.; by Fred J. Shafer, Director, Logistics and Communications Div.

Contact: Logistics and Communications Div.
Budget Function: General Science, Space, and Technology: Telecommunications and Radio Frequency Spectrum Use (258).
Organization Concerned: Department of Defense; Department of Justice; Federal Communications Commission; General Services Administration; Office of Telecommunications Policy.
Congressional Relevance: Rep. Paul N. McCloskey, Jr.
Authority: Federal Property and Administrative Services Act of 1949 (40 U.S.C. 481). Executive Order 115563 U.S.C. 301.

Telecommunications systems are vulnerable to various penetration techniques that may be used for gaining access to the system and intercepting and interpreting communications traffic carried over the system or inserting traffic into the system. Findings/Conclusions: The difficulty of penetration is dependent on such factors as the adequacy of administrative controls, the competence and integrity of telecommunications personnel, the physical security maintained over telecommunications facilities, the technical security resulting from telecommunications technology, and the penetrator's technical knowledge and financial resources. Investigation of abnormalities in telecommunications systems operations is the primary method used for detecting penetrations or attempted penetrations. However, a penetrator may not be identified due to the delays in identifying an abnormality and the investigation of its cause. The General Services Administration and the Department of Defense have issued warnings to civil agencies and military departments and agencies that commercial and most Government telecommunications systems do not provide the degree of security necessary to protect information. Recommendations: Separate computer access controls should be established by the user when computers and associated remote terminal equipment are interconnected through telecommunications systems. Such access controls, if adequate, would increase the difficulty in gaining access to computerized data bases. (Author/SC)

UNITED STATES
GENERAL ACCOUNTING OFFICE

Vulnerabilities Of Telecommunications Systems To Unauthorized Use

Telecommunications systems are vulnerable to various penetration techniques that may be used for (1) gaining access to the system and (2) intercepting and interpreting communications traffic carried over the system or inserting traffic into the system.

The degree of vulnerability depends on various factors. Even though intercepted, sensitive information can be protected against interpretation.

LCD-77-102

MARCH 31, 1977

BLANK

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

LOGISTICS AND COMMUNICATIONS
DIVISION

B-146864

The Honorable Paul N. McCloskey, Jr.
House of Representatives

Dear Mr. McCloskey:

Reference is made to your letter of September 17, 1976, and the subsequent meeting with your staff assistant, Mr. Gordon Earle, on October 6, 1976, concerning vulnerabilities of telecommunications systems. As agreed during the meeting, we obtained information on various techniques and devices used to access telecommunications systems, insert communications into systems, and to intercept and interpret communications traffic; policies and methods applied to detect or prevent unauthorized use of telecommunications systems; and Government pronouncements concerning the vulnerability of information transmitted via telecommunications systems. This information is briefly summarized below and additional information is attached.

Telecommunications systems are vulnerable to various penetration techniques that may be used for (1) gaining access to the system and (2) intercepting and interpreting communications traffic carried over the system or inserting traffic into the system. However, the difficulty of penetration is dependent upon such factors as the adequacy of administrative controls, the competence and integrity of telecommunications personnel, the physical security maintained over telecommunications facilities, the technical security resulting from telecommunications technology, and the penetrator's technical knowledge and financial resources.

Generally, investigation of abnormalities in telecommunications systems operations is the primary method used for detecting penetrations or attempted penetrations. However, a penetrator may not be identified due to the delays in identifying an abnormality and the investigation of its cause.

Although carriers are responsible for unauthorized disclosure of communications, carriers and certain Government telecommunications officials stated that users should have the ultimate responsibility for determining and providing security for their communications. In our study we made no attempt to determine what the relative responsibilities of carriers and users ought to be.

Users may protect their traffic against interpretation through the use of various encoding techniques and devices.

Separate computer access controls should be established by the user when computers and associated remote terminal equipment are interconnected through telecommunications, regardless of the protection provided by the telecommunications system. Such access controls, if adequate, would increase the difficulty in gaining access to computerized data bases.

The General Services Administration and Department of Defense have issued various policies, procedures, and instructions concerning the security and use of telecommunications sytems. Among these are warnings to civil agencies and military departments and agencies that commercial and most Government telecommunications systems do not provide the degree of security necessary to protect information.

This reponse has been based on information furnished by telecommunications carriers, a carrier association, and various Government organizations.

If we can be of further assistance, please advise.

Sincerely yours,

F. J. Shafer
Director

Enclosure

Contents

ABBREVIATIONS

ARS	Advanced Record System
ARPANET	Advanced Research Projects Agency Network
AUTODIN	Automatic Digital Network
AUTOVON	Automatic Voice Network
DOD	Department of Defense
EBS	Emergency Broadcast System
FTS	Federal Telecommunciations System
GSA	General Services Administration
NCIC	National Crime Information Center

GLOSSARY

Access lines	- Circuits from a carrier's end-office center to a terminating point at a customer's premise
Analog	- A telecommunications technique employing continuous electrical signals that vary in some direct correlation to nonelectrical information such as sound or light
Appearances	- Intermediate points for connecting wire pairs along wire and cable routes
Audio amplifier	- A device powered by an external source that produces an amplified reproduction of its input signals
"Blue Box"	- A device that is used to manipulate multifrequency pulsing signals.
Circuit	- A transmission path between one point and another
Classmarking	- User restrictions imposed on access lines at the end-office center
Communications	- All forms of information transmitted from one point (person or equipment) to another
Conductor	- A substance, such as copper wire, that readily conducts electricity
Console	- A panel or groups of panels on which are mounted indicator lights, flip switches, meters, and terminals essential to manual operation or control of electrical equipment
Dedicated circuit	- A circuit designated for sole use by one user or a limited group of users
Demodulator	- A device which receives signals from a circuit and converts them into electrical pulses which may be accepted by terminating equipment

Dial-up	- The use of a dial or push-button device, such as a telephone intrument, to alert certain equipment or persons that a connection/transmission is desired
Digital	- A telecommunciations technique employing discontinuous signals, spaced discrete intervals apart, to represent discrete values for changes in frequency
Drop	- That portion of an access line between an intermediate connecting point (appearance) on or near a customer's premise and a terminating point at a customer's premise
Encoding	- The transformation of information to conceal its actual meaning by means of a secret process or code. The highest level of encoding is referred to as encryption
Facsimile	- The transmission of still pictures, maps, diagrams, and text. Images are scanned by the transmitter and reconstructed by the receiver and duplicated on some form, such as paper
Frequency	- The number of recurrences of a periodic phenomenon in a unit of time specified in cycles per second or "Hertz"
Headset	- A headphone (or pair of headphones) held against the ear. It reproduces the incoming electrical signals as sounds
Hierarchy	- For this report - switching centers classified according to rank and order
Induction	- Indirect acquisition of signals from a magnetic field generated by the varying currents in the electrified conductors of wire pairs
Inductive tap	- A method used to acquire signals from a wire or cable circuit through a device without physical connection
Line-of-sight	- An unobstructed straight line path between two points

Link	- A transmitter-receiver system connecting two locations or the transmission path between those locations
Message format	- Rules of the placement of certain portions of a message, such as transmitter identification codes, destination codes, and message text
Microwave	- A term applied to radio waves of a certain frequency range
Modulator	- A device that receives electrical pulses from terminating equipment and converts them into signals acceptable for transmission
On-line	- For this report - communications between a computer and users' terminating equipment
Optional equipment	- Various equipment ranging from simple and inexpensive electrical measuring equipment to more expensive sophisticated processing equipment
Penetration	- The act of entering a facility, circuit, or network for the purpose of intercepting or transmitting some form of communications
Penetration tools	- Various hand tools, such as wire probes, cutters and strippers, terminal clips, and pliers, that may be used to penetrate wire and cable circuits
Private branch exchange	- For this report - a switching system with manual, semiautomatic, and/or automatic operations normally located on a customer's premise. A switchboard is usually associated with the system
Pulsing	- Variations imposed upon current, voltage, or power normally having constant values
Record	- A grouping of characters, symbols, or marks that form related facts or information and treated as a unit

Routing	- The assignment or selection of circuits or links by which communications are carried to desired destinations
Software	- Coded routines, containing instructions that cause switches to perform desired operations
Switchboard	- An apparatus, normally requiring an operator attendant, located on customers' premises or at carriers' end-office centers to establish connections between users
Terminating equipment	- Equipment, such as telephone instruments and teletypewriters, designed for sending or receiving communications in an environment associated with the work to be performed
Traffic	- The total communications flow, such as conversations, written messages, facsimile and data, in a telecommunications system
Wiretapping	- The act of acquiring communications carried over a wire or cable through direct connection with wire pair conductors or indirectly through inductive pick-up devices

CHAPTER 1

INTRODUCTION

The Communications Act of 1934, as amended, established the Federal Communications Commission (FCC) as the regulatory authority for interstate and foreign commerce in communications by wire and radio. Under this Act, the FCC has established rules and regulations which must be observed by telecommunications carrier companies (hereafter referred to as carriers) in the United States. There are approximately 1,800 carriers operating various types of telecommunications systems in the United States.

The ability to communicate at a distance requires cooperation and coordination among carriers and users for operating the many different telecommunications systems. Telecommunications systems supply the necessary facilities for (1) connecting persons or equipment at the beginning of a call, (2) furnishing a transmission path, and (3) disconnecting them when the call is completed. Generally, the functions of switching, signaling, and transmission are required for electronic communications systems. The control of these functions and network configuration are under the management of carriers.

Carriers' systems include all telecommunications facilities that are managed by the carriers. These include switching equipment and transmission equipment (wire, cable, and microwave).

Users are responsible for controlling physical access to and use of owned or leased terminating equipment, such as switchboards, telephones, teletypewriters, facsimile machines, computer terminals, and other facilities (such as internal distribution lines).

CARRIER SERVICES

Carriers provide switched service, such as the public telephone system that allows system users to be connected with any other user of the same system. Also, carriers provide dedicated service which refers to the exclusive customer use of certain circuits connecting two or more locations. These circuits may be hardwired (nonswitched) or switched between locations. These switched and dedicated services provide transmission capabilities for the following:

--voice (the actual voice or reproduction of the voice carried over voice grade circuits, which are those capable of carrying speech),

--record (teletypewriter, papr tape, magnetic tape, data processing cards, graphics--such as facsimile), and

--data (basic elements of information that can be processed or produced by a computer).

Because the telephone companies have developed their systems primarily for telephone users, their systems are primarily analog systems, which do not require signal conversion during a telephone call. However, there is growing use of digital transmission by the telephone companies and the specialized carriers to transmit digital traffic, such as computer output. Thus, for instance, if the terminals are analog, such as telephones, no conversion is required when transmitted over an analog system, but conversion is required, analog-to-digital for the speech sent and digital-to-analog for the speech received. Vice versa if the terminals are digital, such as computers.

ABUSES OF TELECOMMUNICATIONS

Summary statistics concerning abuses of telecommunications (toll fraud and unlawful interception) were furnished by two carriers and the Federal Bureau of Investigation (FBI). These statistics did not provide a means of identifying duplications, if any; however, they are presented in the following paragraghs to show the existence of abuses.

Two carriers furnished the following toll fraud (unlawful avoidance of toll charges through the use of techniques and devices to circumvent billing) information for the period 1970 through 1975:

Carrier	Arrests	Convictions	Pending
1	58	39	10
2	559	307	Not furnished
Totals	617	346	10

The annual statistics for the same period showed a continuous increase in arrests.

The FBI furnished information only for fiscal year 1975 and 1976. This information on interception of communications (unauthorized disclosures of interstate communications and unlawful wiretapping) is shown below:

Fiscal Year	Investigations	Convictions
1975	Not furnished	25
1976	930	20

GOVERNMENT TELECOMMUNICATIONS

The Government uses a variety of telecommunications services, including the carriers' local and long distance service offerings to the general public and services available through Government systems (generally leased in the continental United States) that have been established to meet specific needs for performing assigned functions and responsibilities. Such services provide capabilities for transmitting voice, record, and data.

Under the authority of Executive Order 11556 (3 U.S.C. 301), the Office of Telecommunications Policy is the primary focal point in the Federal Government for telecommunications policy and coordination. One of it's assigned general functions is to coordinate the telecommunications activities of the Executive Branch and formulate policies and standards, including but not limited to consideration of interoperability, privacy, security, spectrum use, and emergency readiness.

The Federal Property and Administrative Services Act of 1949 (40 U.S.C. 481) gives the Administrator of General Services the responsiblity for procuring and supplying certain Government civil agencies' telecommunications services. Pursuant to this Act, GSA has issued Federal Property Management Regulations including those that set forth standards for establishing privacy and security safeguards over automatic data processing and telecommunications systems.

Pursuant to the Presidental letter of July 1, 1949 (14 F.R. 3699; 3 CFR), the Department of Defense (DOD) and GSA reached an agreement whereby DOD assumed the authority and responsiblity for procuring and managing telecommunications services within DOD. DOD has issued directives and other instructions, including those that set forth policies and procedures covering management of automatic data processing and telecommunications systems.

The Government owns or leases telecommunications terminating equipment connected into carrier and Government systems, whereas, the transmission facilities, between terminating equipment, are normally leased from carriers for Government systems. Some of these transmissions facilities are shared with, and others are physically segregated from, those facilities that carriers use in providing telecommunications service offerings to the general public.

SCOPE

Our inquiry covered industry and Government-wide policies, procedures, and practices used to prevent surreptitious access

to telecommunications systems, insertion of communications into the system, and interception and interpretation of Government communications within the United States. We also reviewed articles published in books and trade magazines, hearings before congressional commissions and committees, and a Government contractor's study concerning vulnerabilities of telecommunications systems to interception.

We interviewed officials and obtained answers to written questions from the Department of Defense, the General Services Administration, the Office of Telecommunications Policy, the Federal Communications Commission, the Federal Bureau of Investigation, the American Telephone and Telegraph Company, the Western Union Telegraph Company, the General Telephone and Electronics Service Corporation, and the United States Independent Telephone Association, all in the Washington, D.C. area. We did not validate the information furnished by these organizations or interpret laws pertaining to unlawful access or attempted access to telecommunications systems, including the interception or interpretation of communications transmitted over telecommunications systems. Also, we did not attempt to obtain information on all Government telecommunications systems. These efforts were not undertaken due to the time constraints for this assignment. However, there was some consistency among the information provided by the various organizations.

Although our inquiry included vulnerabilities of telecommunications used to provide access to computers, we did not investigate the vulnerabilities of computers because we had previously discussed this matter in three recent GAO reports.

CHAPTER 2

VULNERABILITIES OF CARRIERS' SYSTEMS

Carriers have established certain policies and procedures for operating their systems in a manner to minimize penetration. However, a perpetrator with adequate technical knowledge and proper equipment can penetrate carriers' systems and interpret communications thereon. Generally, it is difficult to detect such penetrations. Carriers have advised us of new technologies, being implemented under some long range plans, which are expected to make penetration more difficult.

POLICIES

Carriers have established policies and procedures restricting physical access to plant facilities, requiring employee indoctrination on the requirement for secrecy of communications, and providing for investigations into alleged abuses and employee or user complaints through technical and administrative procedures. According to the carriers and users, the ultimate responsibility for protecting the privacy and security of information transmitted over carriers' systems must be assumed by the users.

SWITCHING

Switching is a technique of making, breaking, or changing connections of transmission paths. There are basically two types of switching used in carriers' systems--circuit and message switching. Circuit switching completes a circuit from sender to receiver at the time of transmission. Message switching is the process of receiving a message, storing it until a suitable outgoing circuit is available, and then sending it on toward its destination. Switching is performed at locations known as switching centers, hereafter referred to as centers. Private branch exchanges are also centers, and for the purposes of this report, under the control of the user. Switchboards associated with such exchanges are discussed in the next chapter.

Generally, carriers employ a hierarchical scheme for switching and, accordingly, rank the centers. For example, the telephone industry ranks its centers as end-office, toll, primary, sectional, and regional centers. At the bottom of the hierarchy, end-office centers provide local service and interconnect customers to long distance service. Toll centers, generally, provide long distance toll charge information service and associated customer billing. Primary, sectional, and regional

centers are switching points (without switchboard operators) that provide automatic circuit switching for the long distance portion of the telephone network.

Carriers' centers may be equipped with semiautomatic or automatic equipment or both. They are operated by personnel, such as console operators, technical and maintenance personnel, and supervisory personnel. Some duties of these personnel require them to access circuits carrying user communications.

For example, some telephone end-office centers have verification circuits. Other end-offices have dial-up access to verification circuits in other centers. These circuits are used for (1) determining whether user access lines are busy or out of order and (2) announcing emergency calls through the interruption of calls in progress. Console operators' access to verification circuits may be gained directly from their consoles or through dial-up to supervisory consoles. To deter improper access by console operators through dial-up, carriers have incorporated some protective features intended to prohibit connections except from designated supervisory consoles. Carriers also use equipment on some verification circuits that scrambles the intercepted conversation which makes it unintelligible to console operators; however, operators can override this equipment for announcing emergencies--at which time a beep tone is audible to the interrupted parties. Carrier officials told us that console operators are instructed that third parties should not be interconnected to verification circuits.

In another example, telephone technical control and maintenance personnel may also require access to user access lines or long distance circuits for performing certain quality control and maintenance testing. A carrier official stated that no audible tones were emitted on user access lines or long distance circuits during such testing. Thus, the vulnerability of improper access to verification circuits or interception of communications from user access lines and long distance circuits, through carrier personnel, is generally dependent upon the competence and integrity of these personnel.

Automatic centers are basically computer operated and under the control of computer software programs. Software programs are usually developed and revised at a central location, but locally implemented at the centers. Remote access to computers is possible for implementing preprogrammed operations, such as routing changes; however, this access does not permit changes or modifications to software programs. Thus, the vulnerability of software programs is dependent upon the competence and integrity of the programming personnel involved.

Signaling

Carrier systems, large or small, require communications between system components Signaling is the intelligence exchanged between system components for establishing connections and supervising transmission paths. Signaling between centers may be divided into two functions--supervision and pulsing. Supervision signals are used for monitoring circuit status, such as idle or busy condition and transmission quality. Pulsing signals are used to assist switching equipment in selecting transmission paths and connecting circuits.

Our inquiry did not identify any vulnerability to penetration through unauthorized use of supervision signals.

There are various types of pulsing signals. One of these, known as multifrequency tone, is vulnerable to manipulation by individuals using multifrequency tone generators, such as "Blue Box" devices costing $50 and up. Our inquiry did not identify any vulnerability to other types of pulse signaling.

Perpetrators use "Blue Boxes" for making long distance telephone calls without cost to themselves. Essentially, perpetrators gain access to a long distance circuit by dialing a toll free number and, before the called number rings, send specific multifrequency tones. These tones cause the switching equipment to disconnect the called number and gives the perpetrator access to long distance circuits. Thus, the perpetrator may place long distance calls without being charged for them. (Further detailed information is contained in testimony presented during the 1975 hearings on surveillance to the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, House of Representatives; and during the hearings conducted by the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance.)

Generally, existing telephone carrier systems allow signaling and user traffic to travel within the same circuit. However, advances in technology are currently being implemented in new equipment installed within the United States. This new technology includes Common Channel Interoffice Signaling (CCIS) which uses separate circuits for signaling and other circuits for user traffic to achieve separation that allows different physical routings of the circuits. Full implementation of this technology is not expected until the 1980s and 1990s.

MICROWAVE

Carriers commonly use terrestrial and satellite microwave links for routing voice, record, or data circuits. Terrestrial microwave uses repeaters, antennas, and associated equipment for line-of-sight telecommunications links. Communications satellites represent a line-of-sight repeater of a specialized kind which permits extension of the terrestrial system over very long distances. Depending on the equipment installed for each microwave link, capacities range from less than 60 to 22,000 circuits, when expressed as voice grade circuits.

Terrestrial Microwave

Generally, the interception of two-way (communciations flowing in both directions between connected parties) voice, record, or data traffic requires capturing transmissions from two directions. Interception and interpretation can be accomplished by a perpetrator with adequate technical knowledge and proper equipment. Interception equipment may be positioned between antenna towers, near an antenna tower, or on both sides of an antenna tower of the targeted microwave links. Equipment used to intercept and interpret transmissions employing analog techniques is generally less sophisticated than the equipment necessary to intercept and interpret transmissions using digital techniques.

Interception of video transmissions requires more selective positioning of special antennas and some additional interception equipment. These additional requirements exist because the ratio of the magnitude between the signal and noise must be greater than for intercepting voice transmissions to achieve a satisfactory picture.

There are several factors that increase the degree of difficulty to surreptitiously intercept individual targeted transmissions. Three of these factors are:

--link capacity (larger as compared to lower capacities will increase intercept difficulty because the perpetrator must isolate the targeted transmission from among a larger number of transmissions).

--circuit routing (alternative routing as compared to dedicated routing will increase intercept difficulty because the targeted transmission will not be limited to the same circuit), and

--type of transmission (digital as compared to analog will increase intercept difficulty because the perpetrator must determine the transmission rate and digital coding scheme used by carriers' equipment or the users' equipment).

Satellite Microwave

Interception of two-way voice, record, or data traffic transmitted via satellite microwave requires capturing transmissions from two directions (up-link and down-link). These interceptions and their interpretations can be accomplished by a perpetrator with adequate knowledge of satellite microwave technology and proper equipment.

There is little differnce between terrestrial and satellite intercept equipment, although antennas required for intercepting satellite microwave are generally larger to acquire acceptable down-link signals. Also, since steerable antennas are required, in some instances, for satellite microwave, they are more expensive. The equipment required for intercepting up-link transmissions must be positioned near the up-link antenna. Equipment required for intercepting down-link transmissions may be placed anywhere within the satellite's radiated beam upon the earth. This could range from several thousands of square miles to nearly a full hemisphere.

The difficulty factors for intercepting individually targeted transmissions, pointed out above under terrestrial microwave, are also applicable to satellite microwave transmissions.

Intercept Equipment Cost

Intercept equipment costs will vary depending on the carriers' facilities targeted, positioning of intercept equipment, and the target information desired by the penetrator. The estimated costs of terrestrial and satellite intercept equipment are shown below.

Intercept Equipment Component	Availability	Estimated Cost	Intercept Effectiveness
Terrestrial Antenna (1 ea)	Commercial	$500 to $2,000	moderate to high
Satellite Antenna (1 ea)	Commercial	$20,000 to $600,000	moderate to high
Receiver with Demodulator (see glossary)	Commercial	$6,000 to $88,000	moderate to high
Other Terminating Equipment	Self made or Commercial	$25 to $15,000	low to high

Detection of Penetration

Visual observation of the penetration equipment is the method used to detect surreptitious interception because, generally, the location of the perpetrator's antenna will not interfere with the transmissions received by the carriers' receiving antenna. Spurious transmissions (inserting traffic into existing microwave links) will usually create interference with the carriers' operating equipment; therefore, such spurious transmissions are detectable.

WIRE AND CABLE

Circuits between end-office centers and users and between end-office centers and other centers are routed over transmission facilities using different types of wire and cable.

A large number of circuits, known as user access lines, will leave the end-office in the form of a main feeder cable containing as many as 100 pairs of wire. The wire pairs are fanned-out through branch feeder cables and finally end as a drop or service wire pair entering a user's premises.

Circuits between end-office centers and other centers, known as trunk circuits, are also routed over wire and cable in some cases.

Commonly used types of wire and cable include:

--open wire (insulated or non-insulated wire conductors),

--multipair cable (cable consisting of many pairs of insulated wire conductors), and

--coaxial cable (cable consisting of one or more tubes surrounded by a pressurized sheath with each tube containing inner and outer conductors).

Interception of communications carried over wire and cable will range from easy to difficult. Open wire may be simply penetrated by directly connecting to the conductors or indirectly through induction (acquisition of signals from a magnetic field generated by the varying currents in electrified conductors, thus not physically contacting the conductors) from the conductors. Multipair cable can be easily penetrated by cutting through the outer sheath and stripping the insulation from targeted wire pairs for direct or inductive connections. Coaxial cable is more difficult to penetrate. A coaxial cable is pressurized and connected to fast-reacting alarms; thus, punctures could be readily detected and, if investigated, any attempted surreptitious penetration should be discovered. Additionally, interception of communications carried over coaxial cable through induction methods is unlikely, since an adequate signal level cannot be acquired.

There are many "appearances" along wire and cable routes. "Appearances" are points where segments of wire and cable are connected together for various purposes, for example, interconnections between main feeder cables and branch feeder cables. Some of these "appearances" are neither physiclly secured nor alarmed (alarms are discussed below under detection of penetration) so they are accessible for penetration. Most of these unsecured or non-alarmed "appearances" are on wire and feeder cable routes.

Basically, carriers use three methods to install wire and cable. These are (1) aerial (wire and cable above the ground, usually attached to poles), (2) buried (cable buried beneath the surface of the ground), and (3) underground (cable placed in underground conduits).

Generally, aerial and buried installations are easier to penetrate than underground installations. Aerial wire and cable, being above ground, are readily available for penetration. Some multipair aerial cables are equipped with alarms, but some of these alarms are not immediately activated. For example, alarms for certain types of insulated cable respond very slowly (up to 4 hours) to punctures. Buried cables are easily identified by cable markers and they can be available for penetration when dug up. Underground multipair cables are also identified by

cable markers, but are not so readily available for penetration because access requires cutting through their conduits.

The user's access line is the only place where all communcations of a specific user is available. The line may consist of open wire, single pair insulated wire, or multipair cable. Thus, they can be rather easily penetrated through wiretapping and remote monitoring. (Further details on wiretapping are contained in the hearings referred to above under signaling.) Therefore, the user's access line is the optimum place for a perpetrator to surreptitiously intercept communications carried over wire and cable. This line also permits spurious transmissions by perpetrators. Detection of penetration is discussed below.

Several factors increase the degree of difficulty to surreptitiously intercept targeted communications or to insert spurious transmissions carried over medium to high density cable routes between centers. Two of the factors are:

--circuit routing (alternate routing as compared to dedicated routing will increase intercept difficulty because the targeted transmission will not be limited to the same circuit), and

--type of wire or cable used (multipair cable as compared to open wire increases the difficulty of interception or insertion; coaxial as compared to multipair cable further increases the difficulty for the perpetrator).

Intercept Equipment Cost

Intercept equipment cost will vary depending upon the carrier facilities, positioning of intercept equipment, and the targeted information desired by the penetrator. The estimated costs of wire and cable intercept equipment are shown below.

Intercept Equipment Component 1/	Availability	Estimated Costs	Intercept Effectiveness
Inductive tap	Commercial	up to $60	very high
Audio amplifier	Commercial	up to $60	very high
Headset	Commercial	up to $60	very high
Penetration tools (various)	Commercial	up to $50	not applicable
Optional equipment	Commercial	$25 to $15,000	low to high

1/ See glossary for definitions of the equipment identified in this column.

Detection of Penetration

Generally, visual observation of the penetration equipment can be minimized by the perpetrator, if the time and place for wire tapping and remote monitoring are judiciously selected. However, carriers employ various testing techniques and alarms to detect problems and , if investigated, may result in identifying penetrations or attempted penetrations. Some of the testing techniques are:

--capacitance testing (the measurement of the electric current flow in a circuit),

--resistance testing (the measurement of the opposition to electric current flow in a circuit), and

--frequency testing (the measurement of the opposition to electric current flow at selected frequencies).

Some of the types of alarms used by carriers are:

--pressurized gas (alarms reacting to decreases in prescribed pressure levels),

--electrical (alarms reacting to changes in prescribed voltages), and

--frequencies (alarms reacting to excessive losses of selected control frequencies).

PERSONNEL

We recognize that certain carrier personnel access various components of a carrier's system while performing their normal duties associated with rendering telecommunications services. Disclosure of any communications obtained during the performance of their duties is subject to the competence and integrity of such personnel. Unauthorized disclosure of interstate communications is subject to severe penalties imposed by the Communications Act of 1934, as amended. Also, carriers' policies and procedures stress security and measures to prevent unauthorized disclosure of intrastate, as well as interstate, communications.

CHAPTER 3

VULNERABILITIES OF GOVERNMENT SYSTEMS

The Government has established certain policies, regulations, and procedures for management of its telecommunications systems and uses certain devices to minimize penetration and safeguard communications. However, a perpetrator with adequate technical knowledge and proper equipment can access Government systems and interpret some communications. The difficulties for penetration and detection vary among the Government systems.

Telecommuncations facilities supporting Government systems are subject to the same vulnerabilities as the facilities supporting carrier systems described in chapter 2. Also, as pointed out in chapter 2, carrier and Government officials have stated that responsibility for protecting information transmitted via telecommunications systems must be assumed by Government users.

We were furnished some additional information concerning certain Government systems during our inquiry. This information--policies, procedures, operating techniques and devices used--pertaining to potential penetration and the deterrents used to increase the difficulty of penetration, is summarized in this chapter.

GENERAL SERVICES ADMINISTRATION

The General Services Administration (GSA) manages a Government system, known as the Federal Telecommunciations Systems (FTS) which provides certain telecommunciations services to Government organizations, during normal and emergency situations. The primary components of the FTS are a voice network and a record and data network.

GSA advised Government organizations, through GSA Bulletin FPMR F-88, dated October 15, 1975, that "*** the FTS normally does not have security features to protect against either loss of, errors in, or interception of information. Therefore, the security and confidentiality of information transmitted over the FTS is not ensured."

FTS Voice Network

The FTS voice network is basically a telephone system leased from carriers, although 216 Government managed switchboards operate in the network. GSA and other Government organizations operate 173 and 43 switchboards, respectively.

GSA has published operating procedures covering the operations of Government switchboards on the FTS voice network. In part, these procedures emphasize the need for maintaining secrecy of communications, outline certain physical security measures for switchboard areas, and instruct operators on emergency interruptions and other switchboard operations. Other GSA publications outline procedures for servicing calls to and from other telephone systems.

Generally, Government operated switchboards in the FTS voice network are similar to those used in public telephone systems. Switchboards have the capability for interconnecting (1) among its users, (2) between its users and other switchboards, and (3) between its users and carriers' end-office centers. Technological advances in telecommunications have diminished, but not eliminated, the roles performed by switchboard operators. Early switchboards required switchboard operators to make all interconnections. Later, dial features were added to permit automatic interconnection by users, but still required switchboard operators to interconnect all incoming calls from other switchboards. Further advances permitted automatic interconnections for incoming and outgoing calls, thereby reducing the switchboard operator's role to providing assistance and performing certain other equipment control functions.

Depending upon the manufacturer, age, and installation, many Government switchboards have capabilities for "executive override" and "busy verification." "Executive override" is a capability whereby a switchboard operator may intercept telephone conversations to advise the connected parties that they are being interrupted or disconnected for an emergency. "Busy verification" is a capability whereby a switchboard operator may access a connection to determine whether or not the connected circuits are in use.

Some Government switchboards do not automatically emit a beeping tone notifying connected parties of an operator's presence on their connection. Also, some switchboards have capabiltiies that allow operators to connect third parties into a circuit already connected between two parties.

Access into the FTS voice network from public or other telephone systems may be accomplished through switchboard operators. However, the operators may request information from callers to assist them in determining the authority for completing calls originating from a non-FTS telephone. Such information includes periodically revised identification codes issued by GSA to Government organizations for internal distribution.

Generally, the vulnerabilities of unauthorized access and interception of communications at switchboards is dependent upon the competence and integrity of the switchboard operators. However, operator competence and integrity are not the only factors concerning vulnerability, since Government organizations may have adequate or inadequate controls for internal distribution of GSA issued identification codes.

Advanced Record System

The Advanced Record System (ARS) is a record and data message system leased from a carrier, although some Government-owned terminating equipment is used. Both leased and Government-owned equipment is installed at various terminal locations throughout the United States, including 72 GSA locations (known as Federal Telecommunications Record Centers) that support several Government organizations in close proximity to each center.

GSA has published policies and guidance concerning the ARS. In part, these policies and guidance require operating personnel to be familiar with operating procedures, emphasize the need for maintaining privacy of communications and physical protection of telecommunications facilities, and advise users of transmission security limitations.

The ARS has two types of switching, circuit switching and message switching. Circuit switching is a feature that permits dial-up, point-to-point connections between terminating equipment. Message switching uses computers between terminating equipment to receive, store, process, and forward record messages.

The computer software programs for message switching centers cannot be remotely altered. Software programs are entered into computers by authorized programmers at each center. Such software programs are reviewed and tested before being placed into operation.

The ARS incorporates two techniques that assist in controlling terminating equipment, "answerback" and "classmarking." "Answerback" is a technique that incorporates predetermined codes, exchanged between sending and receiving equipment, to establish connections. "Classmarking" is a technique, which is an available option to Government users, that permits sending equipment to communicate with only selected receiving equipment.

A perpetrator with sufficient technical knowledge, proper equipment, and knowledge of the answerback code assigned the targeted terminating equipment could intercept messages from and insert messages into the ARS. This could be accomplished by wiretapping a dedicated circuit connecting the targeted terminating equipment and an ARS switch. However, the perpetrator is limited to the classmarking constraints imposed upon the targeted terminating equipment.

A perpetrator may also penetrate the ARS through terminating equipment operating on public record systems, such as the Teletypewriter Exchange Service (TWX) and the International Teleprinter Network (TELEX). This is because some organizations using these systems have also been authorized and provided with an answerback capability permitting interconnection with the ARS; such terminating equipment is known as ARTX or ARTEL terminals. A perpetrator can penetrate the ARS by (1) unauthorized use of an ARTX or ARTEL terminal, (2) wiretapping the access line of an ARTX or ARTEL terminal, and (3) imitating an ARTX or ARTEL terminal by modifying a public record system terminal to incorporate appropriate answerback equipment. In each of the first two situations the perpetrator would be able to insert and receive ARS messages. However, in the third situation the perpetrator could insert ARS messages but could not receive ARS messages because the ARS switching equipment routes messages only over authorized lines.

A perpetrator without access to authorized equipment would have to invest about $1,000 and up for equipment to intercept or insert ARS messages.

DEPARTMENT OF DEFENSE

The Department of Defense (DOD) manages and operates a variety of telecommunications systems to support is national security and military operations. Two of the major DOD systems are known as the Atuomatic Voice Network (AUTOVON) and the Automatic Digital Network (AUTODIN), a record network. Another DOD system is the Advanced Research Projects Agency Network (ARPANET).

Policies

DOD has published policies on safeguarding classified information, protecting this classified information when transmitted over telecommunciations facilities, and prohibiting wiretapping, monitoring, or eavesdropping that does not comply with constitutional and statutory provisions. Also, DOD has instructed its military departments and agencies to remind their users that the FTS, commercial facilities, and

nonsecure DOD systems do not provide the degree of confidentiality necessary to safeguard personal data as required by the Privacy Act of 1974.

DOD officials pointed out that there have been occasional violations of its policies concerning unauthorized interception of communications during the past 2 years. The majority of these violations involved DOD personnel and only violated internal DOD procedures rather than statutory provisions. The remaining violations were referred to the Department of Justice for investigation.

Automatic Voice Network

AUTOVON is the principal DOD long-haul, nonsecure voice network that provides direct distance dialing and circuit switching for voice, graphics and data. Primarily, access to AUTOVON is provided through facilities, such as locally managed switchboards and associated equipment, at DOD installations.

DOD has published policies and procedures governing access, interconnection to other systems, and certain AUTOVON connecting requirements for locally managed switchboards. DOD has also advised operators and users (since AUTOVON is not secure) that care must be exercised to avoid disclosing classified information.

AUTOVON switching equipment is leased from carriers. Although this equipment may be collocated, it is physically separated from the carrier's equipment used for public networks. Interconnection between AUTOVON and the public networks' switching equipment normally requires human intervention.

AUTOVON may be accessed from other Government and public telephone systems through switchboard operators. The operators may request informaton from callers to assist them in determining the authority for completing calls over AUTOVON. Such information includes the caller's name and the destination of the call.

Although an unauthorized individual may successfully imitate a legitimate AUTOVON user without wiretapping, the vulnerabilty to unauthorized access through switchboards is dependent upon the competence and integrity of the switchboard operators.

Although DOD does not expend funds to detect unauthorized AUTOVON accesses, supervisory observations or reviews of certain

traffic information may disclose such accesses. DOD officials stated that only limited measures are taken to detect unauthorized access since AUTOVON in the United States is a nonsecure voice network consisting of leased circuits and switches.

Switchboards

DOD manages various switchboards, having capabilities similar to those discussed under the FTS voice network, that provide internal telephone service and permit access to the AUTOVON, the FTS voice network, and public telephone networks.

Depending upon the manufacturer, age, and installation, some switchboard locations have capabilities, through verification circuits, to announce emergency interruptions and determine whether or not circuits are busy. However, in one instance cited by DOD officials, these verification circuits were moved from switchboard operator consoles to supervisory consoles in 1975. With this arrangement, the switchboard operators do not have the capability to connect any third party into on-going conversations, but such connection could be made through the supervisory console.

Other switchboard locations have manual equipment which permit switchboard operators to directly connect into on-going conversations. To help protect against abuses occurring through this capability, DOD switchboard operators are indoctrinated, trained, and observed by supervisory personnel.

Thus, the vulnerabilities of unauthorized access and interception of communications at switchboards is dependent upon the competence and integrity of the switchboard operators and supervisory personnel.

Automatic Digital Network

AUTODIN is the principal DOD secure switched record network. It functions as a worldwide, high-speed, computer-controlled, general-purpose telecommunications system providing record communication to DOD and other authorized users.

DOD has published policies and procedures governing access, operational and technical control, software management, and transmission security.

The leased AUTODIN switches (hereafter referred to as AUTODIN centers) provide message switching services to users

in the continental United States and Hawaii. Government-owned AUTODIN centers provide similar services to users in other overseas locations. The computer software programs for these centers cannot be remotely altered. All software changes are sent as messages from a central location to each center. Each AUTODIN center has an assigned individual who is responsible for validating changes and maintaining software integrity.

Classmarking used at AUTODIN centers is similar to that used in GSA's ARS.

AUTODIN provides a transmission security feature not normally found in other systems. This feature is the encryption of messages carried over circuits between AUTODIN centers and between AUTODIN centers and most users' terminating equipment. The devices used for encryption are acquired through Government cryptologic organizations and, to our knowledge, are not commercially available.

DOD acknowledges that messages carried over nonsecure circuits are vulnerable to interception, through wiretapping, without detection. A perpetrator may insert messages over such circuits by imitating an authorized user; however, these messages would most likely be rejected for incorrect message format or through certain operating procedures performed at the centers. The estimated cost for the perpetrator's equipment is $1,000 and up.

DOD officials told us there were no known instances of unauthorized access into AUTODIN.

Advanced Research Projects Agency Network

The ARPANET is a telecommunications system designed to provide record and data communications between a variety of geographically separated computers so that computer equipment, software, and data resources could be shared by a wide community of users. The ARPANET circuits are leased from carriers.

The computers are connected into ARPANET through switching equipment (known as interface message processors or terminal interface processors). Such switching equipment is normally owned by certain users and located on their premises. The computers, switching equipment, software, and local circuits are the users' responsibility.

DOD has no knowledge of any unauthorized access and interception of messages carried over the ARPANET. However, DOD recognizes that a perpetrator, if successful in intercepting the transmission path, could monitor communications since ARPANET is not a secure network. Although certain encryption devices will be tested in this network, DOD does not anticipate any growth in secure users since ARPANET may be discontinued in about 4 years.

DOD also recognizes that access to the ARPANET or computers is possible through dial-up to terminal interface processors because such processors do not authenticate callers. For example, a perpetrator could access ARPANET through dial-up using equipment costing about $1,000. However, a perpetrator must have additional knowledge, such as passwords and account numbers to access computers for information processing. Although we did not inquire into the vulnerabilities of computers, such information has been discussed in GAO reports entitled, "Computer-Related Crimes in Federal Programs" (FGMSD-76-27, Apr. 27, 1976) and "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115, Jan. 17, 1977).

FEDERAL BUREAU OF INVESTIGATION

The Federal Bureau of Investigation manages and operates several dedicated telecommuniations systems to provide voice, record, and data communications within the Bureau and between the Bureau and other criminal justice organizations.

National Crime Information Center System

One of the record and data systems managed by the Bureau is a nation-wide, on-line automated information system, known as the National Crime Information Center (NCIC) system. Although the NCIC system is managed by the Bureau, other Federal, state, and local criminal justice organizations participate in its operation.

Complete responsibility for all record transactons (new entries, modifications, and cancellations), including senstive identification information entered into the NCIC system is placed on certain designated Federal or state locations. These records include (1) public information, such as stolen property, wanted persons, and missing persons, and (2) sensitive information that requires protection under the Privacy Act of 1974, such as records on criminal history. Certain records, such as those pertaining to charges of drunkeness and vagrancy, certain public order offenses, and nonspecific charges of suspicion or investigation, are not maintained in the Bureau's computerized files.

Dedicated circuits are used between the Bureau's central NCIC computer and certain NCIC authorized Federal and state locations, known as control terminals. Voice, record, and data communications between state control terminals and local organizations may be transmitted over telephone, teletypewriter and data circuits, or by radio.

Some states have central computerized information systems which are on line through dedicated circuits with (1) the Bureau's central NCIC computer and (2) each state's control terminals. The state control terminals and partcipating local criminal justice agencies have on-line capabilities for entering inquiries and receiving responses for certain record information maintained in the central computerized systems at both state and Federal levels.

Some states do not have on-line computerized systems and do not maintain computerized criminal justice records at the state level. These states use dedicated circuits and software controlled electronic switching equipment to access the Bureau's central NCIC computer. Entering new records and modifying or cancelling existing state records, maintained at the Federal level, is permitted only by state control terminals, through manual connections with the electronic switching equipment. The electronic switching equipment limits access to certain authorized organizations, permits direct administrative communications between these authorized state and local organizations, and permits direct entry of new records, modifying or cancelling existing records, inquiries, and responses.

Some states have manual state control terminals. Interconnections between these state control terminals and the Bureau's central NCIC computer are obtained through dedicated circuits. No computerized state criminal justice records are maintained in these states. Entering new records and modifying or cancelling of existing state records are permitted only through state control terminals. The state control terminals provide services to local agencies through manual intervention.

Other states do not participate in the NCIC system.

The Bureau's central NCIC computer and other computer centers having access to the NCIC system should have certain controls preventing unauthorized access to the system's files and unauthorized use of information obtained from the system's files. Some of these controls are:

--controlling accessibility to criminal history records through computer software,

--recording all entries and responses involving criminal history records (each recording must identify each specific organization entering or receiving information),

--screening and verifying each entry by a computer,

--maintaining adequate physical security to prevent unauthorized personnel from accessing computer equipment and stored records, and

--screening computer center personnel (operating, technical, and maintenance) under the authority and supervision of responsible criminal justice personnel.

Systems security at the Federal level and to the state level is the Bureau's responsibility. Each state is responsible for maintaining system security within its state. It is the Bureau's policy that all control terminals authorized NCIC access are required to have its terminating equipment in secure locations, and only screened personnel are authorized to enter or receive criminal history information. Also, copies of criminal history information obtained through terminating equipment are to be protected from unauthorized use.

Although we did not inquire into the policies and procedures established for controlling access to criminal history records at the state and local levels, such information is discussed in our report entitled, "How Criminal Justice Agencies Use Criminal History Information" (B-171019, August 19, 1974).

We have pointed out some of the vulnerabilities of carrier telecommunciations systems in chapter 2. Also, the GAO report entitled, "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System" (LCD-76-115, January 17, 1977) stated that "*** the state-of-the-art in computer security is such that absolute security has not been achieved." Thus, a perpetrator with adequate knowledge and proper equipment could penetrate the NCIC system for the purpose of retrieving or altering records maintained in state and Federal computerized data bases.

As described in chapter 2, even without penetration of the NCIC data bases, a perpetrator with adequate knowledge and equipment could intercept communications carried over the NCIC circuits. Bureau officials told us that encoding techniques or devices are not used to protect NCIC traffic. They further explained that the expected security benefits obtained though encoding techniques or devices would be minimal because the greatest vulnerability to the NCIC system is the individual terminal operator.

INTERAGENCY

Emergency Broadcast System

The Emergency Boradcast System (EBS) operates at national, state, and local levels. The President may use this system, during grave national emergencies, for promptly addressing the American people. Also, state and local officals may use this system for warnings of natural disasters and other emergency situations.

Executive Order 11490, dated October 28, 1969, assigns emergency preparedness functions to various Federal departments and agencies. EBS is managed by the Federal Communications Commission. Recommendations to the Commission concerning the EBS are made by the National Oceanic and Atmospheric Administration, DOD, and the National Industry Advisory Committee (an ad hoc committee representing the broadcasting industry which makes studies and recommendations for all Commission licensed facilities and regulated services). EBS operations involve the participation of the White House Communications Agency, DOD, GSA, carriers, radio and television networks, wire news networks, and over 9,000 radio and television broadcasting stations.

EBS at the national level, consists of two telecommunciations networks, known as the "500" and "300". The "500" is a teletypewriter system, using dedicated circuits, connecting certain Government organizations with selected offices of radio and television broadcast networks, participating carriers, and wire news networks. The "300" is a telephone system, using dedicated circuits, connecting certain Government organizations with selected offices of wire news networks.

EBS activation at the national level involves separate message transmissions containing certain information over both networks. Each message requires authentication with periodically revised "500" or "300" authentication lists, which are distributed by the Federal Communications Commission, before executing further action.

When participating carriers receive a valid activation message over the "500" network, they reconfigure the broadcast networks for distributing EBS information to affiliated broadcast stations. The activation message transmitted over the "500" network is confirmed over the "300" network with the wire news networks before the activation message is retransmitted to subscribing stations. When the above actions have been accomplished, the EBS is activated.

Unauthorized EBS activation would be difficult because the two networks have different authentication methods.

Surreptitious interception of the communications carried over the activated EBS would not benefit a perpetrator since they are intended for public dissemination.

Secure Voice

It is the policy of the Federal Government to use secure voice systems to protect its voice communications where nationally sensitive matters are involved. An example is the DOD which uses highly sophisticated encryption devices and techniques. Other systems providing varying degrees of security are available.

Use of such systems make interpretation of intercepted communications more difficult than interpretation of unsecured communications. The degree of difficulty of interpreting intercepted secure voice communications is dependent upon the sophistication of the encoding devices, techniques, and controls employed. Inverted speech communications are relatively easy to interpret whereas encrypted communications are extremely difficult to interpret.

CHAPTER IV

CONCLUSIONS

Telecommunications systems are vulnerable to various penetration techniques that may be ued for (1) gaining access to the system and (2) intercepting and interpreting communications carried over the system or inserting communications into the system. However, the vulnerability of telecommunciations systems to unauthorized penetration depends upon various factors such as (1) administrative control, (2) competence and integrity of telecommunications personnel, (3) physical security, (4) technical security, and (5) the technical knowledge and financial resources of the perpetrator.

Administrative control over telecommunciations systems is promulgated through operating policies and procedures. Such policies and procedures include guidance necessary for system operation and maintenance. A by-product of policies and procedures are the practices employed which should result in some protection against unauthorized penetrations. Thus, this factor is dependent upon the adequacy of the established administrative control over telecommunications systems.

Operating personnel (operational, technical, maintenance, and supervisory) perform duties and functions required to provide reliable and quality telecommuncations service. Some of these duties and functions, of necessity, require or permit access to the system by such personnel. The potential for unintentional or intentional (1) unauthorized disclosure of communications or (2) assistance to perpetrators increases as the number of such personnel increases. Thus, this vulnerability factor is heavily dependent on the competence and integrity of such personnel.

Without assistance of or information furnished by telecommunications personnel, perpetrators could gain access to telecommunications facilities if adequate physical security is not maintained over such facilities. A perpetrator may enter Government telecommunications facilities not having adequate physical security and use the terminating equipment without being observed. Also, some appearances along wire and cable routes are not physically protected nor continuously observed, thereby permitting a perpetrator access to such appearances for the purpose of wiretapping. Thus, this vulnerability factor is dependent upon the adequacy of physical security maintained over Government and carrier telecommunications facilities.

Technical security is a by-product of the technology used in telecommunications systems. The technology used is dependent upon various system features, such as:

--type of service (local or long distance; switched or nonswitched; dedicated or general purpose),

--type of communictions (voice, record, data or television),

--type of facilities (wire, cable, or microwave transmission equipment, switching equipment, and terminating equipment),

--type of controls (signaling, testing, alarms, or circuit routing), and

--type of transmission (analog or digital).

These features impact the difficulty and cost to a perpetrator for achieving successful penetration of telecommunications systems. Further, increases in difficulty and cost can be expected as advances in telecommunications technology (such as new signaling techniques and optical transmission) are incorporated in the systems. Thus, the technical security factor impacts the penetration vulnerability of telecommunications systems.

The probability of successfully penetrating a telecommunications system is dependent upon (1) the perpetrator's technical knowledge of the telecommunications facilities and operational techniques and controls used in the targeted system and (2) the financial resources available for acquiring appropriate equipment. Thus, this is another variable factor.

Various abnormalities arise during operation and maintenance of telecommunications facilities. Generally, these abnormalities are first indicated by such means as (1) visual observations of questionable activities, (2) triggered alarms, (3) deviations in testing measurements, (4) discrepancies noted during administrative reviews, and (5) user complaints. Investigations of each indicated abnormality may identify its cause, such as defective alarms, equipment failures, and procedural violations. These same investigations may also result in detecting facility penetrations or attempted penetrations. However, if detected, the perpetrator may or may not be identified due to the time lapse between the penetration and its investigation.

Since users need varying degrees of protection, if any, for their communications, they are in the best position for determining their communications security requirements on the basis of sensitivity, potential threat, potential risk from possible disclosure, and costs for providing protection. Although carriers are responsible for unauthorized disc'osure of communictions, carriers and certain Government telecommunications officials stated that users should have the ultimate responsibility for determining and providing security for their communications. In our study we made no attempt to determine what the relative responsibilities of carriers and users ought to be.

Users can increase the protection against the interpretation of intercepted communications by using various encoding techniques and devices that provide different levels of protection. With proper use, proper accountability, and adequate physical control, encryption techniques and devices provide the highest level of protection. Also, when computers and associated remote terminals are interconnected through telecommunictions, we believe that users should establish separate computer access controls regardless of the protection provided by telecommunications systems. Such access controls, if adequate, would increase a perpetrator's difficulty in gaining access to computerized data bases.