Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db586

Title **FBI File 139-WF-262: Unknown Subject, Possible Access to White House Secure Telephone System, IOC**

Date 1977-05-11

Author(s) FBI

Abstract FBI File 139-WF-262 regarding Draper's claims that it was possible to intercept white house communications. Based on a May 11, 1977 Jack Anderson column that "Rep. McCloskey was advised by a constituent that he had developed a blue box enabling him to tap into secure WH telephone lines." Includes copy of news summary as well as a GAO memo regarding telecom vulnerabilities.

Keywords White House; John Draper; McCloskey; McClosky; Jack Anderson; 139-WF-262; 139-HQ-4991; blue box; wiretapping

Source FBI via FOIA

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

March 31, 2008

Subject: FILE NUMBER WF 139-262

FOIPA No. 1106859- 000

Dear Requester:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552		Section 552a
☐(b)(1)	☐(b)(7)(A)	☐(d)(5)
☒(b)(2)	☐(b)(7)(B)	☐(j)(2)
☐(b)(3)_____	☒(b)(7)(C)	☐(k)(1)
_____	☐(b)(7)(D)	☐(k)(2)
_____	☐(b)(7)(E)	☐(k)(3)
_____	☐(b)(7)(F)	☐(k)(4)
☐(b)(4)	☐(b)(8)	☐(k)(5)
☐(b)(5)	☐(b)(9)	☐(k)(6)
☒(b)(6)		☐(k)(7)

64 **page(s)** were reviewed and ***64*** **page(s)** are being released.

☐ Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:

- ☐ referred to the OGA for review and direct response to you.
- ☐ referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information and Privacy, U.S. Department of Justice,1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001 within sixty days from the date of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☒ See additional information which follows.

Sincerely yours,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

As you have been previously advised, because your FOIA requests are similar in scope and content, that is, they constitute a series of related requests, you are being charged aggregate duplication fees for your requests concerning Blue Boxes, Phone Freaking techniques, and related files. The authority to charge aggregate fees is located in Title 28, Code of Federal Regulations, Section 16.11(h).

Pursuant to Title 28, Code of Federal Regulations, Sections 16.10 and/or 16.49, there is a fee of ten cents per page for duplication. No fees are assessed for the first 100 pages. You have already received your 100 free pages. You are being charged at this time for the enclosed pages. Upon receipt of these documents please make a check or money order payable to the Federal Bureau of Investigation in the amount of $6.40 for 64 released pages. To insure proper identification of your request, please return this letter or include the FOIPA request number(s) with your payment. Failure to pay for this interim release will close your current request as well as any pending FBI FOIA requests from you. Nonpayment will also cause an automatic denial of any future FOIA requests.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

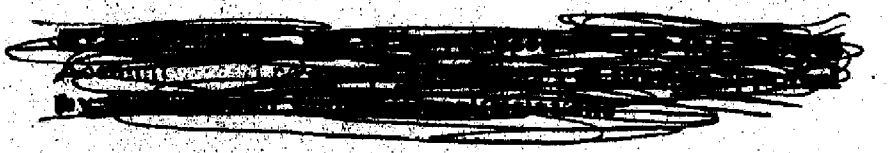
UNSUB;
POSSIBLE ACCESS TO WHITE HOUSE
(Title) SECURE TELEPHONE SYSTEM

(File No.) 139-262*

Item	Date Filed		Disposition
1	5/17/77	U.S. [redacted] (SYM)	

139-262-1A

SEARCHED ____ INDEXED ____
SERIALIZED ____ FILED ____
MAY 17 1977
FBI—WASHINGTON FIELD OFFICE



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

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

ISTICS 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 technic 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 essentia 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 identifiction 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 paragraphs 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 compentence 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 difference 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.

PER

com
dut
Dis
of
suc
cat
Comm
and
auth
comm

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 s required switchboard operators to interconnect all incoming ca from other switchboards. Further advances permitted automatic interconnections for incoming and outgoing calls, thereby reducing the switchboard operator's role to providing assistar 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 identificati codes issued by GSA to Government organizations for interna 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 offical 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 disclosure 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.

AN EQUAL OPPORTUNITY EMPLOYER

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U. S. GENERAL ACCOUNTING OFFICE

THIRD CLASS

The White House News Summary

Wednesday, May 11, 1977

CARTER WARNS NATO ON SOVIET ARMS -- President Carter warned NATO Tuesday it should toughen up to match the Soviet buildup of offensive forces in Europe. Afterwards, he flew home from his first round of summit meetings. "The Soviet Union has achieved essential strategic nuclear equivalence," Carter said to NATO representatives. "Its (European) theater nuclear forces have been strengthened. The Warsaw Pact's conventional forces in Europe emphasize an offensive posture." He suggested that NATO defense ministers begin work next week on improvements "to strengthen the alliance's deterrence and defense in the 1980s." The President also called for a special review of East-West relations, pledged a major U.S. contribution to this study and urged that it be considered at a NATO summit in Washington next spring. (UPI,AP)

COMMITTEE OKS PARTIAL END TO CUBA EMBARGO -- The Senate Foreign Relations Committee voted Tuesday to partially lift the trade embargo against Cuba to permit sales of agriculture, food and medical supplies to that nation. It balked at opening U.S. markets to exports of sugar and other Cuban agricultural products after senators heard arguments that such a step would give away an important bargaining chip in continuing negotiations with the Cuban government. There was no immediate word on when the measure might be taken up by the full Senate. (AP,UPI)

TURKEY WAS ONLY FAILURE -- Carter ended his debut trip abroad hailed as a superstar on the international stage. He said the summit talks have given him "complete faith in the future." The only diplomatic strikeout of the trip was a failure to secure immediate improvement in relations with Turkey. Diplomatic sources said Carter and Turkish premier Suleyman Demirel got "nowhere" in a meeting aimed at healing the rupture in the U.S.-Turkish military alliance. Carter predicted after the meeting that Congress will relax the embargo on arms sales to Turkey. (UPI)

PERSONAL INCOME UP 9.1 PER CENT -- The average American's personal income grew by 9.1 per cent in 1976, well above the inflation rate, the Commerce Department reported Tuesday. Per capita income nationwide increased from $5,903 in 1975 to $6,441 in 1976, according to the report. Another government survey, this one released by the Bureau

Inside —

of Labor Statistics, said Tuesday that consumers are spending more for transportation than for food. The increase in transportation expenditures is caused largely by automobile-related expenditures, government experts said. (AP)

CONSUMER BILL CLEARS NARROWLY -- The House Government Operations Committee approved, 22 to 21, a bill to create a federal consumer protection agency. Passage came after some last-minute lobbying by members of the Carter administration, including Vice President Walter Mondale. The committee rejected Republican attempts to modify key provisions, including an effort to remove the proposed agency's authority to sue other government agencies. (AP, UPI)

SOVIETS REJECT SALT PROPOSALS -- The Soviet Union Tuesday again rejected President Carter's proposals for sweeping cuts in U.S. and Soviet strategic nuclear arsenals. The chief Soviet negotiator in Geneva said any new treaty must be based on the 1974 Vladivostok agreements. (UPI)

BUDGET TALKS STALEMATED -- House and Senate negotiators failed Tuesday to reach agreement on the national defense budget. As a result, they were unable to arrive at a compromise between House and Senate versions of the 1978 federal budget. President Carter asked for $120.1 billion in defense budget authority. The Senate approved $120.3 billion, the House $117.1 billion. Neither side appears willing to budge. "I think we're clearly at a stalemate," said Sen. Edmund Muskie (D-Maine) shortly before negotiators recessed until Wednesday. (UPI)

SOCIAL SECURITY PLAN GETS STIFF CRITICISM -- President Carter's Social Security revision plan got a hostile reception Tuesday from Congress, as skeptical congressmen characterized it as dangerous, a grave error, and politically motivated hocus-pocus. Even some House members who appeared inclined to support parts of the Carter plan questioned whether it had been thoroughly thought out. Several legislators criticized it as being an unreasonable burden for the small business owner. Despite the comments by members of the House Ways and Means subcommittee on Social Security, a subcommittee aide predicted the Carter plan would be approved by the panel. (AP, UPI)

NETWORK NEWS — Tuesday evening, May 10, 1977

NBC Nightly News

CUBA--Senate Foreign Relations Committee votes to allow Cuba to buy medicine, agricultural products in U.S., but not to export sugar here. The administration stayed neutral in this move, but is "not displeased." A/:35

SUMMIT--Carter attends NATO meeting in London, discusses the defense of Europe. Callaghan welcomes NATO ministers, shows sense of relief that Protugal has joined the ranks of democracies, NATO nations agree to build up their alliance. Callaghan leaves no doubt Carter passed his international test, says Carter is "proving a true leader of the western world." Carter leaves London with

a new sense of the U.S. role, one that is "sobering but also very gratifying." Says he found a greater depth of friendship to U.S. than he had anticipated. He heads home hailed as a man who has infused a new spirit in troubled Europe. The exhausting nature of the meetings shows as Callaghan muffs introduction of Portugal's new president. The summit was generally thought to have been a success, was "certainly" a personal success for Carter. A,C/6:00

SPECIAL--NBC broadcasts a summit special at 11:30 p.m. Tuesday. A/:12

INCOME--Commerce Department says personal income increased faster than consumer prices last year. Per capita income is up from $5,900 to $6,400. A/:25

OIL--Oil well troubleshooter Red Adair testifies before House committee, says more safety training could lessen blowouts, which are due mostly to "the human factor." He doesn't want federal inspectors interfering with his work. C/1:55

MURDER--Three suspects are arrested in the murder of millionaire widow. Car dealer got suspicious when one suspect paid cash for an $11,000 car. C/2:17

CRAWFORD--Joan Crawford dies of a heart attack at 69. A/:27

PLANE--Eastern Airlines will test-fly four foreign-made airbuses for four months. A/:15

DIPPERS--A special report on double-dipping. Some prominent members of Congress are double-dippers. Some critics of move to cut the practice warn it could spur military unionization, say it is unfair to cut pensions of folks currently drawing both pension and federal salaries. But cost of double-dippers' pensions is approaching $1 billion annually. C/4:30

STORM--Northeast digs out from freak snowstorm that left thousands without electricity, raised fears for the apple crop, and destroyed cloth shelters for Rhode Island shade tobacco, used to wrap fine cigars. Cs/3:14

PHARAOH-- Mummy of Ramses II returns to Cairo, cured of fungus infestation, is welcomed with full military honors. A/:35

LONDON--Jeff Carter took time out to visit a traditional British pub. Billy would have approved. C/1:15

CBS Evening News

CARTER--Carter leaves London at conclusion of summit that was a personal success for him. He seems to have charmed and impressed the other heads of state. At speech before NATO leaders, Carter sets to rest fears that the U.S. might ask other governments for greater contributions to NATO defense forces. He asks that NATO resources be spent with greater efficiency. Carter says he feels his presence at the conference has brought renewed confidence for Western Europe. Callaghan says Carter is "a breath of fresh air to the western world." A/2:40

FICA--Carter Social Security proposal runs into immediate trouble in the House. Rep. Bill Archer (R-Tex) calls it hocus-pocus. Of eight Democrats who heard Califano's arguments for it, five say they have serious doubts about the proposal. C/1:30

WHEAT--Winter wheat crop will probably be better than expected, but still six per cent below last year. Commodity prices have fallen recently. Big corn crop also expected. C/2:05

COTTON--Proposed government regulations on cotton dust, aimed at preventing brown lung disease, run into stiff criticism at Lubbock, Tex., hearing. Rep. George Mahon (D-Tex) says proposed OSHA rules are based on flimsy evidence and could drive growers out of business. C/1:40

CONSUMER--Consumer Protection Agency proposal still alive by one vote. A/:15

INCOME--Personal income up 9.1 per cent. It's ahead of the inflation rate. American families spend more on transportation than food. A/:32

MAIL--Post office charges that AMA failed to pay postage bill for its magazine. AMA is willing to pay part of bill. A/:17

ARMS--Guideline on arms sales prepared for Carter would allow unlimited arms sales to NATO countries and a few others, but would provide for sales on a case-by-case basis for the rest of the world. The guidelines raise worries that the U.S. might cut arms sales to Israel as pressure for Mideast agreement. C/1:25

AIR FORCE--Senate panel investigates potential fast one by the Air Force. Why did the Air Force go ahead with computer system after Congress ordered it stopped? Major general denies attempt to flim-flam Congress. C/1:35

ULSTER--Ian Paisley, attempting to spark new interest in strike, is arrested. C/ 1:25

CUBA--Senate Foreign Relations Committee agrees to partial lifting of U.S. trade embargo against Cuba. A/:17

FLOOD--2,200 West Virginia families may have to stay in temporary housing for up to two years in the wake of recent flood. A/:15

SEABROOK--Half of Seabrook demonstrators still in jail. Background on the Clamshell Alliance, which has organized the Seabrook protest. C/3:15

STANFORD--Stanford University students protest university investments in companies which operate in South Africa. A/:17

SNOW--Snow knocks out electricity to thousands in New England. A/:17

KENNEDY--New York Daily News hires Caroline Kennedy as copy person. A/:07

CRAWFORD--Joan Crawford dead of heart attack. A/:07

STEEL--Six per cent boost in steel prices seems certain. A/:16

STOCKS--Stocks up. A/:17

COMMENT--Eric Sevareid says Carter dominated the public sessions of the summit but not the private work session. Summit ultimately focused on human freedom: interdependence has become a must. 2:10

ROSALYNN--Rosalynn Carter has meeting on aging, entertains senior citizens in White House. C/1:55

ABC Evening News

CARTER--Callaghan calls Carter "a breath of fresh air" for the West; Carter aides believe he has been "smashing." Carter tells NATO he wants mutual force reductions with Warsaw Pact countries, but will increase U.S. support for NATO if force reduction efforts fail. A,C/2:50

PRESS--Carter will hold a press conference at 2:30 p.m. Thursday. A/:12

CRAWFORD--Actress Joan Crawford, 69, dies. A/:27

SECURITY--House Ways And Means Committee urges caution on Carter Social Security reforms. A/:27

ADAIR--Red Adair "disappoints" House committee liberals and defends oil industry for its safety, environmental record in off-shore drilling. C/1:56

LEUKEMIA--The plight of Army vet Paul Cooper, 44, believed dying of leukemia because of exposure to experimental nuclear blasts, has caused the CDC to begin the search for others involved in the 1950's Army experiments. CDC also considering new restrictions on exposure to radiation. C/4:05

CANCER--National Cancer Institute orders strict, new guidelines on breast X-rays on women under 50. A/:24

WIDOW--Three arrested for the murder/robbery of the wealthy Indianapolis widow. C/1:58

SPRING--Massive power blackouts plague New England following snowstorm.. A/:27

INCOME--Personal income rose 9.1 per cent in 1976. A/:20

STOCKS--Dow up, 3.05 points. A/:15

STRIKE--Police thwart Protestant strikers in rural Northern Ireland village. A/:27

SUMMIT--Correspondent says the summit was good for Carter domestically by demonstrating he can "hold his own" with world leaders. Another correspondent says Carter established himself as an "international figure," and made steps toward peace in the Mideast in his meeting with Assad. A,Cs/2:03

ISRAEL--Israel fears Assad meeting indicates tilt toward Arabs. A/:12

COMMENT--Howard K. Smith notes that allied reaction to the Zaire situation bodes well for increasing NATO's strength. 1:55

WARNKE--Warnke flies to Geneva to resume SALT talks. A/:23

CUBA--Senate Foreign Relations Committee backs easing of Cuban trade embargo. A/:18

ROSALYNN--Rosalynn Carter will visit seven Latin American countries next month. A/:22

PEOPLE--Caroline Kennedy begins work at New York Daily News, mummy of Ramses II returned to Egypt, King Hussein linked romantically to Floridian. A/1:02

CRICKET--Harry Reasoner expounds on the differences between cricket and baseball. A/:58

*****

The White House Communications Agency will play back a composite of Tuesday evening's network news shows Wednesday at 9:30 a.m. on channel 6 and at 12:30 p.m. on channel 2. The video tape will last approximately 30 minutes.

*****

See back page for morning news.

DAILY PRESS

JUDGE DENIES INDIANS' CLAIMS TO IOWA LANDS -- The Omaha Indian Tribe's claim to title of 2,900 acres of Iowa farmland has been denied by federal Judge Andrew Bogue. The Indians' claim is based on 100-year-old documents which show their reservation lands to be bounded by the Missouri River. The tribe claims that the river has shifted its course to the south and east, leaving portions of their reservation land on what is now the Iowa side of the river. Along with his ruling, which the Indians will appeal, Bogue wrote that the Congress should redefine Indian boundaries by longitude and lattitude and said the Indians deserved compensation for their loss. (Des Moines Register)

ISRAEL WILL NOT WITHDRAW TO 1967 BORDERS -- Israeli Foreign Minister Yigal Allon will inform Secretary of State Cyrus Vance that Israel must retain large portions of occupied Arab lands to insure defensible borders, the Los Angeles Times reported. The Israelis plan to hold onto captured lands in the Jordan Valley and the Gaza Strip, the Times said. Israeli sources have indicated that Israel will reject any peace plan that does not cede the desired captured lands to Israel, including suggestions that UN observer posts or Israeli outposts beyond new political borders could allow Israel to return to its pre-war borders.

CHILDREN PRESCRIBED TETRACYCLINE DESPITE RISKS -- Many doctors are ignoring seven-year-old warnings against the antibiotic tetracycline and prescribing it to children despite risk of serious harm, the Journal of the American Medical Association reported. The report was based on a study of nearly 59,000 Tennessee youngsters -- thousands of whom had been given tetracycline, a drug found to have harmful effects in children under 8 years of age. According to studies begun in 1970, the powerful antibiotic can cause a lessening of bone growth, serious stomach infections, rashes and other problems in young children. (Chicago Sun-Times)

DROUGHT CAUSES MAJOR FISH KILL -- Thousands of fish died in early May when the Walla Walla River in Washington became too shallow for the fish to survive, the Washington Ecology Department said. "There were ditches along the river in spots where you could wade knee-deep in dead fish," said a department official. Heavy pumping for irrigation left the drought-crippled river with too little water for the fish to live, he said. Although this was the first major fish kill reported this year, the official said he expected "several more" because of the drought.

New calculations of the snowpack in Washington's mountains indicate there will be even less water for power generation and irrigation than had been forecast. Snowpack measurements, which had measured at 40 to 50 per cent of normal in the April report of the Washington Soil Conservation Service, were estimated at as low as 12 per cent of normal in the May report. The State Energy Office, meanwhile, announced there is a 55 per cent chance electricity cutbacks will be ordered by August. (Seattle Times)

PBB-LACED BEEF STILL ON MARKET -- Michigan residents have eaten more than one million pounds of PBB-tainted beef in the first four months of 1977, according to testing at slaughterhouses and to consumption figures from the beef industry. The contamination turned up mostly in hamburger from dairy cattle. Tests at Michigan slaughterhouses have shown that low levels of PBB are still appearing in dairy cattle this year -- nearly four years after the 1973 feed accident igniting the Michigan PBB disaster. A Michigan state senate committee is considering a bill that would reduce the level of PBB permitted in meat. (Detroit Free Press)

AD CAMPAIGN IRKS MONTANANS -- An advertising campaign by the Old West Regional Commission to lure foreign businesses to "the Energy States of America," the upper Midwest, has been disavowed by Montana Gov. Thomas L. Judge and a number of environmental officials. The Old West Regional Commission, representing Montana, North and South Dakota, Nebraska and Wyoming, is a federally funded agency promoting commercial development in those states. The ads, which appeared in London newspapers, described the region as "rich in coal, oil, natural gas and water...all the energy you'll ever need..." Judge, who is a member of the commission, said he was "really outraged" when he learned of the campaign, which he called "misleading and deceptive." (Missoula, Mont., Missoulian)

COMMENTARY

SUMMIT -- "Some future adjustments and compromises on the specifics of the plan may be necessary. But at least the free world's major powers are agreed on the crucial point--that unemployment and inflation must be fought at the same time, with equal vigor. Mr. Carter had considerably less success preaching the gospel of nuclear restraint to his associates, especially West German Chancellor Helmut Schmidt...Further proliferation of nuclear arms is a threat to all mankind. We should make the most earnest effort to bring our allies around to a proper appreciation of the risks, and the necessity for imposing effective controls over dangerous technology." (New York Daily News)

"Was the Downing Street summit a success? More or less, mostly more." (Philadelphia Inquirer)

"The most significant thing about the Big Seven's economic summit is the essentially conservative economics that came out of it." (Chicago Tribune)

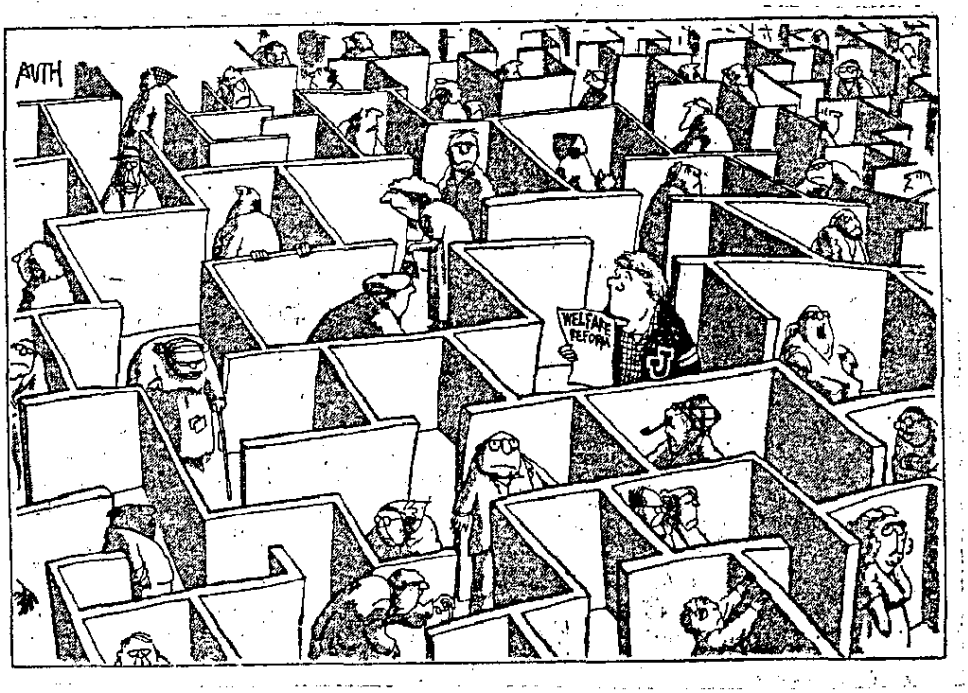
"President Carter's first major effort in foreign affairs, the strategic arms limitations proposals presented to the Russians by Secretary of State Cyrus Vance, appeared to be a fumble. But his second venture, the presidential trip to Europe for summit meetings mostly on economic matters, appears to be a resounding success." (Atlanta Constitution)

"By participating in the London summit with his counterparts from the other industrial nations, President Carter has launched an important international effort. His presence at the meetings underlines and reaffirms America's commitment to its friends of long standing and particularly its ties with Europe... Jimmy Carter has won impressive public support in his first three months in office. His direct manner may be able to work the same wonders at the summit... With luck, he may be able to set the stage for real international progress in the future." (Boston Globe)

"If there is a political lesson to be drawn from the leaders with whom Jimmy Carter (met) in London, it is that the diverse winds that blow across West Europe are making it harder to govern from the middle of the road...The question is whether the eclipse of political moderation will threaten the stability of West European nations. If the impatience of voters transfers the reins of power to the hands of more extreme figures of the left and right and if the extreme leaders are unable to furnish solutions, an inclination will clearly develop to say that democracy has failed and firmer forms of leadership are needed." (Charles Bartlett in the Chicago Daily News)

ETHICS -- "The proposed new ethics law would also make it more difficult for officials to go to work for private interests soon after leaving government service. Amen to that," wrote Newsday. The editors also supported the proposed special prosecutor's office and urged that Congress be included in the jurisdiction of the special prosecutor.

"We like what Carter is doing, and we believe that Congress will accommodate him by enacting his recommendations into law at this session. It is more than a probability that senators and representatives who are still choking on the bland dose of reform that they were willing to swallow will be happy to dose the administration with much stronger medicine." (Los Angeles Times)



"President Carter, in a special message, has called on Congress to approve strict ethical standards for the executive branch and the means to deal with high-level scandal in his or any future administration. We endorse the direction in which Mr. Carter seeks to go." (Philadelphia Inquirer)

"President Carter acted wisely this week in calling for a sweeping ethics law," the Chicago Sun-Times wrote. The paper added that "Carter's bill could be strengthened by adding proposals from a bill sponsored by Senators Charles H. Percy (R-Ill.) and Abraham Ribicoff (D-Conn.)" that would extend the provision to cover all three branches of government. "By acting on Carter's plan," the Sun-Times said, "Congress could complete this year's historic reforms."

SOCIAL SECURITY -- "There is no question but that Social Security is in trouble. And it needs help. But the answer cannot be, forever and forever, higher and higher taxes...These (administration) reforms should be considered long and carefully, before working Americans are weighted down even more with taxes -- and before the United States of America becomes even more of a socialistic, collectivistic, welfare nation." (Atlanta Constitution)

WELFARE -- "President Carter can back away from some of his proposals and produce sound reasons to do so -- dropping his $50 tax rebate plan, for example. But his unexpected willingness last week to delay welfare reform -- and to delay for four years more -- is an unacceptable retreat." (Chicago Sun-Times)

"Welfare legislation affects so many people in so many different ways that slow, deliberate action is not a bad idea, so long as there is steady progress toward the ultimate goal -- an efficient and fair welfare program that will not be unnecessarily burdensome to the taxpayers." (Houston Chronicle)

"Because of its unfettered growth, its inequities and the absence of the essential element -- incentive -- this nation's welfare non-system has become its own worst enemy and a frustration for its people. The Carter administration will not solve this vexing problem overnight. But placing essential stress on the element of self-reliance is a commendable first step." (Columbus, Ohio, Dispatch)

"It must be hoped that the Carter administration's setting of deadlines does not hamper its efforts to do the job right. It has taken us many years to get into the tangle we now deplore, and a 'crash' program that overlooks crucial details could leave us with a shambles in which the really needy are needlessly short-changed -- or afflicted by legions of indifferent bureaucrats -- while the sharpies and angle-shooters find ways to enrich themselves at the public trough." (Sarasota Herald-Tribune)

ENERGY -- "The standby gas tax may have more symbolic than real value. Like a pair of blinders, it would help keep attention focused on the goal of cutting consumption. If the proposal is stripped from the President's energy package, few drivers will feel as much compulsion to do their part to reduce unnecessary consumption as they would with the standby tax staring them in the face. If nothing else, the gas tax merits more detailed study and analysis than the knee-jerk reaction it has received to date." (Akron Beacon Journal)

"More is being made of an apparent discrepancy between two assessments of world oil reserves than should be...It is far safer in planning for the future to rely on known reserves rather than an unknown source which might be produced in the future. The more conservative estimates of the CIA provide a sound basis for planning now." (Americus Times-Recorder)

"The first auto sales report issued since President Carter outlined his energy plan was alarming to the domestic auto industry and the men and women who work in it. Foreign cars scored a sales gain of 62.2 per cent in April and topped the 200,000-unit level for the first time...President Carter should worry more than a little about what he has done to the car market and the auto worker. And the auto industry should spend more time finding out why its smallest cars are not putting up a better show against Volkswagen, Toyota, Datsun, Honda and the like." (Detroit News)

"I'm going to take Carter's energy crisis seriously when the biggest lie of all is abandoned -- the deception about energy costs. It does the President no good at all to talk about shortages when he and the Congress keep the price of energy in the United States far below the world market price...Right now it is clear that neither the President nor the Congress is going to take seriously the responsibility to stop the 'lie' of subsidized energy. Until they do that, we ought not to take them seriously." (Andrew Greeley in the Chicago Tribune)

NUCLEAR -- "It is all very well for us to lay down restrictions and to threaten penalties for nuclear development abroad, but it is not very well for our allies. And they are not about to accept our restrictions, though they make polite little gestures of compliance with our wishes or of acquiescence to international treaties...If the President persists in his present nuclear policy vis-a-vis our allies, he can wreck the Atlantic Alliance." (Alice Widener in the Columbus, Ohio, Dispatch)

"Mr. Carter seems to be signaling that he is willing to seek accommodation, though he is still committed to containment of plutonium technology...Perhaps a nuclear energy summit conference, similar to the series of economic summits, would be useful in mending this split over the atom." (Houston Post)

RIGHTS -- "Secretary of State Cyrus Vance's recent statement on the Carter administration's controversial human rights policy is a useful redefinition of the President's attempt to sell American ideals in the real world where the need for them is great but the supply rather scant. And it could enable the whole approach to human rights to survive and to work...But it would have been more reassuring if Vance had included in his call a commitment to act

with the utmost restraint and caution when recommending assistance to governments with doubtful records on human rights. That, it seems, has been the missing element in American foreign policy." (Boston Globe)

"Secretary of State Cyrus Vance's recent speech calling for realism and flexibility in applying the human rights policy is a welcome modification." (Philadelphia Bulletin)

"Vance's speech does not by any means suggest a lessening of administration determination to press for the advancement of human rights wherever possible. It does, happily, indicate a new recognition of diplomatic limits and the dangers of trying to act as a moralistic scold for the rest of the world." (San Antonio Light)

"How Carter and other top administration officials can continue to avert reproachful glances from the doings of the Park regime is puzzling. What is needed, perhaps, is a stern policy that would make U.S. aid to South Korea contingent on restoration of the fundamental liberties Park treats with contempt." (Des Moines Register)

VOTE REFORM -- "The Carter administration's proposal that voters in federal elections be registered at polling places on election day is fraught with danger...Now, at last, the Justice Department has acknowledged essentially the same thing in an internal memorandum...The present system of preregistration does not need changing, especially for the inherently risky proposition now under consideration." (Houston Chronicle)

"If Congress is bent on passing this kind of legislation, it must incorporate into it every possible safeguard...The need for this hurry-up registration still has not been proved by its supporters." (Memphis Commercial Appeal)

DOUBLE-DIPPING -- "President Carter is reportedly planning to introduce legislation to curb the practice of double-dipping -- military retirees taking government jobs -- because it is 'unfair' to Social Security recipients who are deprived of benefits if they earn more than a minimum amount of outside income... Actually, the just course would be to revise the Social Security laws to allow people to receive benefits they and their employers have purchased without regard to whatever income they earn." (Orlando Sentinel-Star)

"What Carter's legislation will entail is not precisely known. But it should be fair. If the employes want to keep their government jobs, their military retirement pay should be reduced or deferred until their government careers end." (Austin American-Statesman)

ABC Good Morning America

ANDERSON--Jack Anderson reported that a constituent of Rep. Pete McCloskey (R-Cal.) has developed a "blue box" which enables him to tap into secured White House telephone lines. McCloskey agreed to test his constituent's device, and, after dialing the proper sequence of numbers, found he was talking on a confidential White House phone line, Anderson said.

NBC Today Show

BLUMENTHAL--Treasury Secretary W. Michael Blumenthal said in an interview that tapping general tax revenues and increasing employers' contributions to bolster the Social Security fund would have only a minimal effect on the average citizen's taxes and on the rate of inflation.

Commenting on the London summit, Blumenthal said the results were both substantial and psychological. He said the main accomplishment of the meeting was that the seven leaders now understand each other and are committed to working together to solve their common problems. Blumenthal said the psychological results "are not to be underrated," explaining that confidence in the economy is a major factor in determining the health of the economy.

The actions taken on human rights and nuclear proliferation did not represent failures for President Carter, Blumenthal said. He said there was no expectation on the Americans' part of having a statement on human rights written into the communique of an economic conference. The nuclear proliferation question is a "difficult issue," Blumenthal admitted, but he added that the leaders "achieved a lot" in gaining a "basic understanding" of each others' position on the issue.

Complaint Form
FD-71 (Rev. 7-21-67)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: ☐ Negative ☐ See below

b6
b7C

Subject's name and aliases

Unknown Subject, Possible access to White House Secure Telephone System

Character of case

IOC

Complainant

SA [redacted]

Complaint received

☐ Personal ☑ Telephonic Date 5/11/77 Time

Address of subject

Complainant's address and telephone number

White House

Subject's Description

Race	Sex	Height	Hair	Build	Birth date and Birthplace
Age	☐ Male ☐ Female	Weight	Eyes	Complexion	

Scars, marks or other date

Facts of complaint

SA [redacted] advised "White House News Summary" dated May 11, 1977 reflected a television statement by Jack Anderson that Rep. McCloskey was advised by a constituent that he had developed a blue box enabling him to tap into secured WH telephone lines.

SA [redacted] obtained a copy of the above news summary

139-162-2

Action Recommended

O & A

[redacted]

[redacted]

FIELD OFFICE

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/20/77

KENNETH NELSON, Assistant Director, Logistics and Communications, Government Accounting Office (GAO), 44 G Street, N.W., was interviewed and provided the following information:

Congressman PAUL N. MC CLOSKEY sent a letter to GAO dated September 17, 1976, concerning vulnerabilities of telecommunications systems. Attached to the letter was a communication prepared by a constituent of Representative MC CLOSKEY. Mr. NELSON allowed the interviewing agent to read the letter and attachment but would not provide a copy. The information in the attachment was written by [redacted] Mr. NELSON stated [redacted] was also known as [redacted] was supposedly serving time in jail for use of a "blue box." [redacted] set out the ease with which access could be gained to various telecommunications systems.

b6
b7C

[redacted] indicated in the letter that he could be contacted "via [redacted]"

Mr. NELSON provided a copy of GAO report LCD-77-102 titled "Vulnerabilities of Telecommunications Systems to Unauthorized Use," which was based upon Mr. MC CLOSKEY's letter of September 17, 1976.

Mr. NELSON had previously mailed a copy of the GAO report to Federal Bureau of Investigation (FBI) Headquarters.

Interviewed on 5/12/77 at Washington, D. C. File # WFO 139-262

by SA [redacted] :nas Date dictated 5/13/77

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/20/77

b6
b7C

[redacted] United States Representative PAUL MC CLOSKEY (California), [redacted], was contacted concerning an article in "The White House News Summary," May 11, 1977, regarding a "blue box." He was advised of the Federal Bureau of Investigation's (FBI) interest in matters concerning the Interception of Communication Statute. He provided the following information:

During a constituent meeting in California (date not provided), a constituent provided Congressman MC CLOSKEY with a memorandum titled "New Techniques of Tapping Phones and Access to Computers." He spoke briefly to the Congressman and told him he had been prosecuted for using a "blue box" and the Congressman believed the man to be awaiting sentencing. The constituent wanted the Congressman to be aware of the easy access to various items.

The memo included a statement that ". . . the special Hot Line to the President is 800-424-9337," and "Phone freaks have been able to penetrate this system and talk to key government personnel and the President."

In order to verify this information, the Congressman's California staff telephoned the 800 number which was answered by White House Staff. They would not answer any questions and referred them to White House Communications. Congressman MC CLOSKEY's staff spoke with Lieutenant Colonel ED NELSON, United States Army, Operations Officer for White House Communications. NELSON advised that the above number is a number that the White House Staff uses when traveling. It is not a secure telephone line. According to [redacted], NELSON indicated they have received several crank calls over the years and are considering having the number changed.

As a result of the memorandum, Congressman MC CLOSKEY called GAO and requested an investigation. GAO has since written a report titled "Vulnerability of Telecommunications Systems to Unauthorized Use," March 31, 1977.

Interviewed on 5/12/77 at Washington, D. C. File # WFO 139-262

by SA [redacted] :nas Date dictated 5/12/77

The GAO report is a public document, however, JACK ANDERSON is quoting it as classified according to [redacted] An associate of JACK ANDERSON called Congressman MC CLOSKEY's office for a copy of the report. b6 b7C

The identity of the above constituent was requested and [redacted] stated that it was the policy of the Congressman's office not to reveal the identity of a constituent when information of this nature is provided.

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/20/77

1

KENNETH NELSON, Assistant Director, Logistics and Communications, Government Accounting Office (GAO), 44 G Street, N.W., was interviewed and provided the following information:

Congressman PAUL N. MC CLOSKEY sent a letter to GAO dated September 17, 1976, concerning vulnerabilities of telecommunications systems. Attached to the letter was a communication prepared by a constituent of Representative MC CLOSKEY. Mr. NELSON allowed the interviewing agent to read the letter and attachment but would not provide a copy. The information in the attachment was written by [redacted] Mr. NELSON stated [redacted] was also known as [redacted] was successfully serving time in jail for use of a 'blue box.' [redacted] set out the case with which access could be gained to various telecommunications systems. b6 b7C

[redacted] indicated in the letter that he could be contacted via [redacted]

Mr. NELSON provided a copy of GAO report LCD-77-102 titled 'Vulnerabilities of Telecommunications Systems to Unauthorized Use,' which was based upon Mr. MC CLOSKEY's letter of September 17, 1976.

Mr. NELSON had previously mailed a copy of the GAO report to Federal Bureau of Investigation (FBI) Headquarters.

Interviewed on 5/12/77 at Washington, D. C. File # WFO 139-5

by SA [redacted] :mas Date dictated 5/13/77

FD-302 (REV. 11-27-70)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/20/77

1

[redacted] United States Representative PAUL MC CLOSKEY (California), [redacted] was contacted concerning an article in "The White House News Summary," May 11, 1977, regarding a "blue box." He was advised of the Federal Bureau of Investigation's (FBI) interest in matters concerning the Interception of Communication Statute. He provided the following information:

b6
b7C

During a constituent meeting in California (date not provided), a constituent provided Congressman MC CLOSKEY with a memorandum titled "New Techniques of Tapping Phones and Access to Computers." He spoke briefly to the Congressman and told him he had been prosecuted for using a "blue box" and the Congressman believed the man to be awaiting sentencing. The constituent wanted the Congressman to be aware of the easy access to various items.

The memo included a statement that ". . . the special Hot Line to the President is 800-424-9337," and "Phone freaks have been able to penetrate this system and talk to key government personnel and the President."

In order to verify this information, the Congressman's California staff telephoned the 800 number which was answered by White House Staff. They would not answer any questions and referred them to White House Communications. Congressman MC CLOSKEY's staff spoke with Lieutenant Colonel ED NELSON, United States Army, Operations Officer for White House Communications. NELSON advised that the above number is a number that the White House Staff uses when traveling. It is not a secure telephone line. According to [redacted], NELSON indicated they have received several crank calls over the years and are considering having the number changed.

As a result of the memorandum, Congressman MC CLOSKEY called GAO and requested an investigation. GAO has since written a report titled "Vulnerability of Telecommunications Systems to Unauthorized Use," March 31, 1977.

Interviewed on 5/12/77 at Washington, D. C. File # WFO 139-262-6

by SA [redacted] nas Date dictated 5/12/77

The GAO report is a public document, however, JACK ANDERSON is quoting it as classified according to [redacted]. An associate of JACK ANDERSON called Congressman MC CLOSKEY's office for a copy of the report. b6 b7C

The identity of the above constituent was requested and [redacted] stated that it was the policy of the Congressman's office not to reveal the identity of a constituent when information of this nature is provided.

UNKNOWN SUBJECT;
POSSIBLE ACCESS TO THE
WHITE HOUSE SECURE TELEPHONE SYSTEM
INTERCEPTION OF COMMUNICATIONS

On May 11, 1977, the following item appeared in "The White House News Summary":

"ABC Good Morning America Jack Anderson reported that a constituent of Rep. Pete McCloskey (R-Cal) has developed a "blue box" which enables him to tap into secured White House telephone lines. McCloskey agreed to test his constituent's device, and, after dialing the proper sequence of numbers, found he was talking on a confidential White House phone line, Anderson said."

b6
b7C

On May 12, 1977, [redacted] United States Representative McCloskey, was interviewed by the Federal Bureau of Investigation (FBI) and the results of that interview follow:

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

6 - Bureau
1 - San Francisco (Info)
1 - WFO

DPH:nas
(8)

139-262-7

Searched

xxx

5/20/77

TO: DIRECTOR, FBI

FROM: SAC, WFO (139-262)([redacted]C) b6 b7C

UNSUB;
Possible Access to the
White House Secure
Telephone System
IOC

Enclosed herewith for the Bureau are the original plus five (5) copies and for San Francisco one (1) copy of a letterhead memorandum (LHM) captioned as above.

WFO indices reflected a reference to [redacted]

This information is in a WFO letter and LHM dated 8/29/72 to Acting Director (100-448910), titled Youth International Party (YIP) IS-REV ACB (OO:NY). The LHM contains information regarding a [redacted]

UACB, WFO will conduct no active investigation. WFO not submitting a copy of the GAO report to the Bureau inasmuch as a copy has previously been mailed by GAO.

2 - Bureau (Enc. 6)
1 - San Francisco (Enc. 1)(Info)
(1) - WFO

DPH:nas
(4)

CONSOLIDATED
Date: JUN 8 1977
Initials:

DESTROY: 10 YRS.
RETAIN:

139-262-8

X AIRTEL

2/23/79

TO: SAC, SACRAMENTO [redacted]

FROM: SAC, WFO [redacted]

[redacted] aka

[redacted]

FBW

(OO: SACRAMENTO)

b2
b6
b7C

ReWFOteletype and telephone call to Sacramento on 2/22/79.

Enclosed for Sacramento is pertinent information concerning captioned subject obtained from Washington Field Office (WFO) file 139-262.

Searched .....
Serialized .....
Indexed .....
Filed .....

2 - Sacramento (Encs. 3)
2 - WFO (1 - 139-262)

CTB:mer
(4)