Ronald Reagan Presidential Library
Digital Library Collections

This is a PDF of a folder from our textual collections.

Collection: Roberts, John G.: Files
Folder Title: Computer Crime (2 of 2)
Box: 11

To see more digitized collections visit:
https://reaganlibrary.gov/archives/digital-library

To see all Ronald Reagan Presidential Library inventories visit:
https://reaganlibrary.gov/document-collection

Contact a reference archivist at: reagan.library@nara.gov

Citation Guidelines: https://reaganlibrary.gov/citing

National Archives Catalogue: https://catalog.archives.gov/

THE WHITE HOUSE

WASHINGTON

February 7, 1984

MEMORANDUM FOR D. EDWARD WILSON, JR.

FROM: JOHN G. ROBERTS JGR

SUBJECT: Computer Security Information

The attached correspondence, together with a copy of my interim reply, is submitted for reference to the appropriate entities in the Office of Administration. It goes without saying that we make no recommendation whatsoever concerning the products described in the correspondence and accompanying materials.

Many thanks.

THE WHITE HOUSE

WASHINGTON

February 7, 1984

Dear Ms. Skorupski:

Thank you for your January 26 letter to the President, and the accompanying material concerning computer security devices marketed by your company. In that letter you asked that the material be directed to the person responsible for computer security at the White House.

I have referred the material to the White House Office of Administration. That office is responsible for procurement matters, and the officials in that office will give the material you submitted every appropriate consideration.

Thank you for the supportive comments in your letter.

Sincerely,

John G. Roberts
Associate Counsel to the President

Ms. Jean M. Skorupski
International Mobile Machines
Corporation
1755 Jefferson Davis Highway
Suite 505
Arlington, Virginia 22202

JGR:JGR:aea 2/7/84
cc: FFFielding/JGRoberts/Subj/Chron

ID # 201760 CU

CR009

JV

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET

☐ O - OUTGOING
☐ H - INTERNAL
☐ I - INCOMING
Date Correspondence Received (YY/MM/DD) / /

Name of Correspondent: Jean M. Skorupski

☐ **MI Mail Report** **User Codes: (A)** _____ **(B)** _____ **(C)** _____

Subject: Computer Security

ROUTE TO:		ACTION		DISPOSITION		
Office/Agency	(Staff Name)	Action Code	Tracking Date YY/MM/DD	Type of Response	Code	Completion Date YY/MM/DD
CW	Holland	ORIGINATOR	84/10/02			/ /
		Referral Note:				
WHTR		R	84/10/02		S	84/10/12
		Referral Note:				
			/ /			/ /
		Referral Note:				
			/ /			/ /
		Referral Note:				
			/ /			/ /
		Referral Note:				

ACTION CODES:
A - Appropriate Action
C - Comment/Recommendation
D - Draft Response
F - Furnish Fact Sheet to be used as Enclosure
I - Info Copy Only/No Action Necessary
R - Direct Reply w/Copy
S - For Signature
X - Interim Reply

DISPOSITION CODES:
A - Answered
B - Non-Special Referral
C - Completed
S - Suspended

FOR OUTGOING CORRESPONDENCE:
Type of Response = Initials of Signer
Code = "A"
Completion Date = Date of Outgoing

Comments: _____

Keep this worksheet attached to the original incoming letter.
Send all routing updates to Central Reference (Room 75, OEOB).
Always return completed correspondence record to Central Files.
Refer questions about the correspondence tracking system to Central Reference, ext. 2590.

5/81

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF ADMINISTRATION
Washington, D.C. 20503

February 13, 1984

MEMORANDUM FOR THOMAS K. LEWIS, JR.
DIRECTOR
AUTOMATED SYSTEMS DIVISION

FROM: D. EDWARD WILSON, JR. D.E.W.Jr.
GENERAL COUNSEL

SUBJECT: Computer Security Information

Attached for your information is a January 26, 1984 letter from Jean M. Skorupski, the Washington Representative of International Mobile Machines Corporation concerning computer security. She has asked that her information be sent to the person responsible for computer security at the White House. You will note that John G. Roberts, Associate Counsel to the President, has responded on behalf of the President; no additional correspondence is required by OA.

This material is sent to you for your information only; as John states in his cover memorandum to me, no recommendations are made whatsoever concerning the products described in the correspondence and accompanying material.

cc: John G. Roberts ✓

THE WHITE HOUSE

WASHINGTON

April 16, 1984

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS

SUBJECT: Computer Crime Legislation
H.R. 5112

Assistant Attorney General McConnell has asked for your assistance in expediting OMB clearance of Justice's proposed "Federal Computer Systems Protection Act of 1984." According to McConnell, Congressman Hughes plans to move computer crime legislation through Congress this year, and will mark up his own bill on April 26 unless the Administration submits its bill before that date.

The Justice proposal (attached) would add new sections to Title 18, making it a felony to knowingly devise or intend to devise a scheme to defraud, obtain money by false pretenses, or embezzle and to access or attempt to access certain computers in connection with the scheme. The computers covered by the bill are those owned by, contracted to, or operated for the U.S. Government or a federally-insured financial institution, or those operating in interstate commerce. The bill authorizes a penalty of up to five years imprisonment and/or a fine of up to $50,000 or double the amount derived from the crime, whichever is greater. The bill also proscribes damage to covered computers or computer programs, and for a violation of this provision authorizes the additional penalty of forfeiture of the computer used to commit the crime. This additional penalty is designed to deter the junior high school computer whizzes who break into the Los Alamos computers and do such things as change the targets on all our nuclear missles to various points in New Jersey.

McConnell submitted the Justice proposal to OMB on March 16, 1984, so OMB can hardly be accused at this point of inordinate delay in clearing the bill. Nonetheless, in light of the imminence of action on this topic in Congress, McConnell would like to have the package cleared by April 20. I have reviewed Justice's proposed bill and have no objections. The attached draft memorandum for Jim Murr notes that we have no objection to the bill and also nudges OMB to expedite clearance.

Attachment

THE WHITE HOUSE

WASHINGTON

April 16, 1984

MEMORANDUM FOR JAMES C. MURR
CHIEF, ECONOMICS-SCIENCE-GENERAL GOVERNMENT
BRANCH, OFFICE OF MANAGEMENT AND BUDGET

FROM: Orig. signed by FFF
FRED F. FIELDING
COUNSEL TO THE PRESIDENT

SUBJECT: Computer Crime Legislation
H.R. 5112

Counsel's Office has reviewed the "Federal Computer Systems Protection Act of 1984," submitted by the Department of Justice for clearance on March 16. We have no objection to the bill, the section-by-section analysis, or the transmittal letter to the Speaker. We are advised by the Department of Justice that imminent Congressional action on other, flawed computer crime bills makes it highly desirable to submit an Administration proposal by April 20, and we would accordingly appreciate expediting clearance of the Justice proposal.

FFF:JGR:aea 4/16/84
cc: FFFielding/JGRoberts/Subj/Chron

THE WHITE HOUSE

WASHINGTON

April 16, 1984

MEMORANDUM FOR JAMES C. MURR
CHIEF, ECONOMICS-SCIENCE-GENERAL GOVERNMENT
BRANCH, OFFICE OF MANAGEMENT AND BUDGET

FROM: FRED F. FIELDING
COUNSEL TO THE PRESIDENT

SUBJECT: Computer Crime Legislation
H.R. 5112

Counsel's Office has reviewed the "Federal Computer Systems Protection Act of 1984," submitted by the Department of Justice for clearance on March 16. We have no objection to the bill, the section-by-section analysis, or the transmittal letter to the Speaker. We are advised by the Department of Justice that imminent Congressional action on other, flawed computer crime bills makes it highly desirable to submit an Administration proposal by April 20, and we would accordingly appreciate expediting clearance of the Justice proposal.

FFF:JGR:aea 4/16/84
cc: FFFielding/JGRoberts/Subj/Chron

ID # 221976 CU

JV

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET

TR003

John

☐ O - OUTGOING
☐ H - INTERNAL
☐ I - INCOMING
Date Correspondence Received (YY/MM/DD) 1 1

Name of Correspondent: Robert A. McConnell

☐ **MI Mail Report** **User Codes:** (A) _____ (B) _____ (C) _____

Subject: Computer Crime Legislation (H.R. 5112)

ROUTE TO:		ACTION		DISPOSITION		
Office/Agency	(Staff Name)	Action Code	Tracking Date YY/MM/DD	Type of Response	Code	Completion Date YY/MM/DD
CU Holland		ORIGINATOR DN	84/04/11			1 1
CWAT 18		Referral Note:				
		D DN	84/04/12		S	84/04/18
		Referral Note:				
			1 1			1 1
		Referral Note:				
			1 1			1 1
		Referral Note:				
			1 1			1 1
		Referral Note:				

ACTION CODES:
A - Appropriate Action
C - Comment/Recommendation
D - Draft Response
F - Furnish Fact Sheet to be used as Enclosure
I - Info Copy Only/No Action Necessary
R - Direct Reply w/Copy
S - For Signature
X - Interim Reply

DISPOSITION CODES:
A - Answered
B - Non-Special Referral
C - Completed
S - Suspended

FOR OUTGOING CORRESPONDENCE:
Type of Response = Initials of Signer
Code = "A"
Completion Date = Date of Outgoing

Comments: Mar 28 84 Robert McConnell memo to FFF also attached

Keep this worksheet attached to the original incoming letter.
Send all routing updates to Central Reference (Room 75, OEOB).
Always return completed correspondence record to Central Files.
Refer questions about the correspondence tracking system to Central Reference, ext. 2590.

5/81

U.S. Department of Justice
Office of Legislative Affairs

221976 cu

Office of the Assistant Attorney General

Washington, D.C. 20530

11 APR 1984

M E M O R A N D U M

TO: Fred F. Fielding
Counsel to the President
The White House

FROM: Robert A. McConnell
Assistant Attorney General
Office of Legislative Affairs

SUBJECT: Computer Crime Legislation

To update my memorandum of March 28 (copy attached) on the subject draft legislation, Chairman Hughes postponed until April 26 the Subcommittee mark-up of his computer crime bill, H.R. 5112. In doing so, his staff indicated the desire of the Subcommittee to have our detailed views on computer crime legislation before proceeding. It was made clear, however, that Hughes wants to move computer crime legislation this Congress and that he cannot wait past April 26 for our input.

As there is so much media and Congressional interest in computer crime, and as we agree that legislation in this area would be of some value, this could be a very good issue for the Administration and for law enforcement if we can be cleared to submit our draft bill to the Congress. It does not seem unrealistic to suggest April 20 as a target date for submission to the Congress of a computer crime bill.

Your assistance in expediting Administration review of our computer crime proposal will be deeply appreciated.

Attachment

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 28, 1984

M E M O R A N D U M

TO: Fred F. Fielding
Counsel to the President
The White House

FROM: Robert A. McConnell
Assistant Attorney General
Office of Legislative Affairs

SUBJECT: Need for Administration Clearance of Anti-Terrorism and Computer Crime Legislative Proposals

Two proposed Administration legislative initiatives presently under review within the Administration merit priority attention. The anti-terrorism legislative package, which I know Lowell has discussed with you, is the more urgent of the two. Since I know that the demands on your time and attention are great I thought a single memo with current concerns and status would be of assistance to you. We need assistance!

The President announced in his State of the Union Address that he would be submitting a comprehensive anti-terrorism legislative package "shortly". Nine weeks have since elapsed and no legislative package has been submitted. In those weeks Congressional interest has grown, concern over the Olympics has spread and such concern raises the issue of terrorism, and legislative time for action is getting alarmingly short.

I. Anti-Terrorism Legislation.

In summary, the anti-terrorism legislation is a five-part package developed by the Departments of Justice and State which would: (1) establish federal criminal jurisdiction over conspiracies to murder, maim or kidnap persons overseas where an act in furtherence of the conspiracy is carried out in the United States; (2) prohibit public or private technical assistance to foreign terrorist groups or to foreign nations which support terrorism;

(3) authorize payment of rewards for information concerning domestic or foreign terrorism; (4) strengthen federal kidnapping laws consistent with the International Convention on Hostage-Taking; and (5) strengthen federal aircraft piracy laws consistent with the Montreal Convention concerning the safety of civil aviation. The Departments of Justice and State have been in complete accord on this legislation since early December.

The only issue which has held up submission of the anti-terrorism legislative package to the Congress is CIA concern over the conspiracy part of the package. CIA, joined by DOD, wants an express exception for intelligence agency operations. Obviously, this would be an incredible "red flag" as such an exception would be widely perceived as an authorization for U. S. intelligence agencies to conspire to murder, maim and kidnap persons overseas as they see fit.

In an effort to accommodate the concerns of CIA, we have moved the conspiracy provision of the package to the Neutrality Act chapter of the Code; we have consistently interpreted the Neutrality Act as not applying to properly authorized government activities. Assistant Attorney General Steve Trott of the Criminal Division has also provided CIA with a letter memorializing our interpretation of the conspiracy title as not applying to properly authorized government activities. While we were initially led to believe that either of these measures would satisfy CIA, the Agency subsequently concluded that both steps were insufficient and that the only solution is an express exception or deletion of the conspiracy part from the package.

The Departments of Justice and State have endeavored to secure a resolution of this single outstanding issue. Reportedly Director Stockman has now also joined us in urging a resolution. He apparently shares our concern that further delay will seriously jeopardize any prospects for enactment of needed anti-terrorism measures this year and our view that further delay may be embarrassing to the President.

Indeed, we have been told that Stockman has written to the President requesting a decision. I thought you should know of that action if it is true. Despite these efforts, no resolution of the issue has been forthcoming. A copy of our anti-terrorism package is attached for reference purposes.

II. Computer Crime Legislation.

On March 16, 1984, after much discussion and a growing "Hill" interest, the Department submitted to OMB a draft bill to strengthen federal criminal laws governing computer-related crime. In summary, our proposal would establish clear federal jurisdiction over computer-related theft, fraud and sabotage to the extent that such offenses involve use of facilities of interstate commerce,

federal computers, or computers of federally regulated financial institutions. Our proposal would also establish misdemeanor sanctions for "electronic trespasses" or unauthorized access, involving federal computers or computers of federally regulated financial institutions. Of course, we do not propose exclusive federal jurisdiction over any of these offenses. Rather, our jurisdiction would be concurrent with that of state and local law enforcement.

As the result of media attention to the computer crime issue, there is considerable support in the Congress for computer crime legislation. The House has already approved a bill, H.R. 3075, requiring a "study" of computer crime as it affects small business and a similar Senate bill, S. 1920, is receiving consideration. In addition Representative Nelson's bill H.R. 1092 has 118 cosponsors and the Congressman is pushing very hard with some effect. Unfortunately, we feel Nelson's bill has serious defects which an Administration bill could remedy. Moreover, Rep. Bill Hughes has introduced a combination credit card fraud - computer crime bill, H.R. 5112, and plans to process quickly his bill through his Subcommittee on Crime and the House Committee on the Judiciary.

As conditions are present for enactment of computer crime legislation this year, it is important that we have a cleared Administration position available if the Administration is not to be "left behind" and we are to influence the form of any computer crime legislation which is approved. We need to move quickly.

It should be noted that our draft bill proposes no study of computer crime and does not get into the computer security issues which have been addressed by OMB and the Department of Commerce with respect to encouraging those who operate computer systems to take advantage of available technology designed to prevent unauthorized access to computer systems. Rather, our bill is limited to establishing federal criminal sanctions for particular types of computer-related crime. Because of this relatively narrow focus, it would seem that we could secure clearance of our proposal without substantial delay. Attached for reference purposes is a copy of our computer crime package.

While this issue is not as incredibly time sensitive as terrorism I felt you needed to be aware of the situation. It does have a time sensitivity and we could use your assistance in expediting the process.

Attachments

ID # 212552 CU

JV

CM009

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET

☐ O - OUTGOING
☐ H - INTERNAL
☐ I - INCOMING
Date Correspondence Received (YY/MM/DD) 1 1

Name of Correspondent: Robert A. McConnell

☐ **MI Mail Report** **User Codes: (A)** _____ **(B)** _____ **(C)** _____

Subject: A legislative proposal entitled the "Federal Computer Systems Protection Act of 1984"

ROUTE TO:		ACTION		DISPOSITION		
Office/Agency	(Staff Name)	Action Code	Tracking Date YY/MM/DD	Type of Response	Code	Completion Date YY/MM/DD
CU	Holland	ORIGINATOR	84/03/16			/ /
		Referral Note:				
CU	AT18	A	84/03/18			/ /
		Referral Note:				
			/ /			/ /
		Referral Note:				
			/ /			/ /
		Referral Note:				
			/ /			/ /
		Referral Note:				

ACTION CODES:
A - Appropriate Action
C - Comment/Recommendation
D - Draft Response
F - Furnish Fact Sheet to be used as Enclosure
I - Info Copy Only/No Action Necessary
R - Direct Reply w/Copy
S - For Signature
X - Interim Reply

DISPOSITION CODES:
A - Answered
B - Non-Special Referral
C - Completed
S - Suspended

FOR OUTGOING CORRESPONDENCE:
Type of Response = Initials of Signer
Code = "A"
Completion Date = Date of Outgoing

Comments: _____

Keep this worksheet attached to the original incoming letter.
Send all routing updates to Central Reference (Room 75, OEOB).
Always return completed correspondence record to Central Files.
Refer questions about the correspondence tracking system to Central Reference, ext. 2590.

5/81

ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGISLATIVE AFFAIRS

Department of Justice
Washington, D.C. 20530

16 MAR 1984

212552

Honorable David A. Stockman
Director, Office of Management
and Budget
Washington, D.C. 20503

Dear Mr. Stockman:

Enclosed are copies of a proposed communication to be transmitted to the Congress relative to: a legislative proposal entitled the "Federal Computer Systems Protection Act of 1984."

Please advise this office as to the relationship of the proposed communication to the Program of the President.

Sincerely,

(Signed) Robert A. McConnell

Robert A. McConnell
Assistant Attorney General

Enclosures

To coordinate clearance contact Maria Walicki, 633-3916, OLA.

DOJ

OLA-6A
REV 12-23-76

Office of the Attorney General
Washington, D. C. 20530

Speaker of the House
House of Representatives
Washington, DC 20515

Dear Mr. Speaker:

Enclosed for your consideration and appropriate reference is the Federal Computer Systems Protection Act of 1984, a legislative proposal that would amend the United States code to proscribe computer fraud and other crimes involving computers.

Computer related crime is a growing problem in the government and private sector. The prosecution of persons engaged in computer related crime is difficult under current federal criminal statutes. Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other federal offense. Even if an approach is devised that apparently covers the illegal acts, it still must be treated on an untested, untried basis of prosecution in the federal trial courts. The federal courts, the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes using them, require a clear statement of definition and proscribed action.

This act is designed to fill a potentially serious gap in existing federal law by providing a specific sanction for computer related crime. The act makes it a felony to knowingly devise or intend to devise a scheme or artifice to defraud, or for obtaining money or property by false or fraudulent pretences or representations, or to embezzle, steal, or convert the property of another, and to access or attempt to access certain computers for these purposes.

The act also proscribes the knowing and unauthorized damaging or destroying of a computer, computer program, or data contained in a computer. This applies to computers owned by, under contract to, or operated for or on behalf of the United States Government, a financial institution or those operating in or using a facility of interstate commerce.

Finally, the act specifies that whoever intentially and without authorization accesses a computer owned by, under contract to, or operated for or on behalf of the United States Government or a financial institution, shall be guilty of a misdemeanor and shall be fined not more than $25,000 or imprisoned for not more than one year, or both.

Enclosed for your review is a section-by-section analysis of the proposal.

The Office of Management and Budget has advised that there is no objection from the standpoint of the Administration's program to the submission of this legislation to the Congress and that its enactment would be in accord with the program of the President.

Sincerely,

William French Smith
Attorney General

Enclosures

A BILL

To amend Title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1984."

SEC. 2. (a) Chapter 47 of Title 18, United States Code, is amended by adding at the end thereof the following new section:

"§ 1028. Computer fraud and abuse.

"(a) Whoever having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or convert to his use or the use of another, property not his own, for the purpose of executing such scheme or artifice or embezzlement, theft or conversion or attempting to do so, knowingly accesses or attempts to access a computer, shall, if the computer --

"(1) is owned by, under contract to, or operated for or on behalf of --

"(A) the United States Government; or

"(B) a financial institution, or

"(2) operates in, or uses a facility of,

interstate commerce,

be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever knowingly and willfully without authorization damages, destroys or attempts to damage or destroy a computer described in subsection (a)(1) and (2) or knowingly and willfully without authorization damages or attempts to damage any computer program, or data contained in such computer shall be fined not more than $50,000 or imprisoned not more than five years, or both.

"(c) Whoever intentionally and without authorization accesses a computer as defined in (a)(1), or a computer system or computer network including such computer, shall be guilty of a misdemeanor and shall be fined not more than $25,000 or imprisoned for not more than one year, or both.

"(d) Whoever violates any provision of paragraph (a), (b) or (c) shall forfeit to the United States any interest acquired or maintained in any computer and computer software, which has been used to commit the violation. Upon conviction under this section, the court shall authorize the Attorney General to seize all property or other interest declared forfeited under this section upon such terms and conditions as the court shall deem proper. If a property right or other interest is not exercisable or transferable

for value by the United States, it shall expire, and shall not revert to the convicted violator. The United States shall dispose of all such property as soon as commercially feasible, making due provision for the rights of innocent persons.

"(e) DEFINITIONS. -- For the purpose of this section the term --

"(1) 'computer' means an electronic, magnetic, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"(2) 'computer system' means a set of related connected or unconnected computers, computer equipment, devices and software;

"(3) 'computer network' means two or more interconnected computers, computer terminals or computer systems.

"(4) 'financial institution' means --

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal Home Loan Bank system and any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to Section 15 of the Securities and Exchange Act of 1934;

"(5) 'property' includes, but is not limited to, financial instruments, information, including electronically processed or produced data, and computer program and computer software in either machine or human readable form, computer services and any other tangible or intangible item of value;

"(6) 'financial instrument' means any check, draft money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card or marketable security, or any electronic data processing representation thereof;

"(7) 'computer program' means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which permits the

functioning of a computer system in a manner designed to provide appropriate products from such computer system;

"(8) 'computer software' means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system;

"(9) 'computer services' includes but is not limited to computer time, data processing, and storage functions;

"(10) 'United States Government' includes a branch or agency thereof;

"(11) 'access' means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network; and

SEC. 3. The table of sections of Chapter 47 of Title 18, United States Code, is amended by adding at the end thereof the following:

"1028. Computer fraud and abuse."

SECTION-BY-SECTION ANALYSIS

Section one of the bill contains its short title: The Federal Computer Systems Protection Act of 1984.

Section two of the bill adds a new section 1028 to title 18 of the United States Code proscribing computer fraud and other crimes involving computers. The proposed new section contains five subsections, (a)-(e).

Proposed subsection (a) makes it a felony to knowingly devise or intend to devise a scheme or artifice to defraud, or for obtaining money or property by false or fraudulent pretenses or representations, or to embezzle, steal or convert the property of another, and to access or attempt to access certain computers for these purposes. The term "access" is defined in proposed subsection 1028(e)(11) and means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, a computer system, or computer network. Subsection (a) is designed to plug a potentially serious gap in existing federal law by providing a specific sanction for computer related crime. Presently there is no federal law directly related to such an offense. When computers are used in federal crimes such as an interstate fraud scheme, any federal response must be based on a theory of prosecution that can be made to fit the facts of the case. Since computers open up entire new areas for crimes the facts of a particular case may not always fit. For example, computers are repositories of

tremendous amounts of valuable information and data but placing a value on this material should it be stolen is often difficult or impossible.

The proposed subsection is drafted in language that is taken from the mail fraud (18 U.S.C. 1341) and wire fraud (18 U.S.C. 1343) statutes to the maximum extent possible. It is intended that the extensive body of law that has been developed interpreting these statutes apply to the new subsection 1028(a).

The penalty for a violation of subsection 1028(a) can extend to five years' imprisonment and a fine of $50,000 or double the amount derived from the offense, whichever is greater.

The subsection only applies if the computer accessed or to which access is attempted is in one of three categories. They are computers owned by, under contract to, or operated for or on behalf of the United States government; computers owned by, under contract to, or operated for or operated for or on behalf of a "financial institution;" and computers operating in or using a facility of interstate commerce. The term "financial institution" is defined in subsection 1028(e)(4) and includes all banks insured by the Federal Deposit Insurance Corporation, Federal Reserve member banks, federally insured savings and loan associations and credit unions, and certain federally insured or registered brokerage firms.

Coverage of all computers operating in or using a facility of interstate commerce such as, for example, telephone lines if used for an interstate call, extends federal jurisdiction

over a very large number of computers. Such jurisdiction would be concurrent with that of the states although subsection 1028(a) is deliberately drafted to allow the option of federal investigation and prosecution in appropriate cases such as where state laws are inadequate or where investigation in several states is required.

Subsection 1028(b) sets out another felony offense involving computers. It proscribes the knowing and unauthorized damaging or destroying of a computer, computer program, or data contained in a computer. The computers covered are those in the three categories listed in subsection 1028(a). The conduct aimed at here would include the physical destruction of or damage to a computer itself (the hardware), and damaging a computer program or data in the computer. "Computer program" is a defined term in subsection 1028(e) and means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system. The penalty for a violation of the subsection extends to five years' imprisonment and a $50,000 fine. Attempts to violate the subsection are also covered.

Subsection 1028(c) would make it a misdemeanor punishable by up to one year's imprisonment and a $25,000 fine to intentionally and without authority access a computer owned by, under contract to or operated for or on behalf of the United States or a financial institution, or a computer system or computer network

including such a computer. The term "computer system" is defined in subsection 1028(e). It means a set of related connected or unconnected computers, computer equipment, devices and software. The term "computer network" is also defined in subsection 1028(e). It means two or more interconnected computers, computer terminals, or computer systems.

The conduct proscribed in subsection 1028(c) is akin to a trespass onto someone else's property. A person who rummages through the information contained in a computer, computer system, or computer network -- for example by accessing the computer system or network through his home computer -- causes the same sort of harm as an intruder who clandestinely enters a person's home to look through the contents of the owner's personal records and documents. Subsection (c) applies whether or not anything of value, such as information, is taken.

Subsection 1028(d) provides for the forfeiture to the United States of the interest acquired or maintained in any computer or computer software used in the offense by a person convicted of a violation of subsection (a), (b), or (c). A forfeiture provision provides for significant deterrence to potential violators above the threat of a prison sentence and fine. Some courts can be expected to be reluctant to give prison sentences or meaningful fines in some cases involving computers, particularly those in which the defendant has merely made an unauthorized access to a computer system or network by means of his home computer. The

possibility that such a person might have to forfeit his expensive home computer should dissuade him from such unauthorized rummaging.

The subsection sets out a criminal forfeiture and the intention of the government to seek a forfeiture, which is left to the discretion of the prosecutor, must be alleged in the indictment or information. If the defendant is found guilty of the offense, a special verdict must be returned concerning the forfeiture allegations. At that point the government could seize the computer or the defendant's interest in the computer software. Prior to this time the court may enter a restraining order or require the defendant to post a bond to guard against unauthorized disposition of the forfeitable property. Although usually the computer itself would be forfeited, the subsection also refers to "computer software" to cover the situation where a person has an interest in a computer program that has been developed and sold to facilitate a fraud scheme or unauthorized access to a computer system or network. "Computer software" is defined in subsection 1028(e) as a set of computer programs, procedures and associated documentation concerned with the operation of a computer system. Of course subsection (d) only applies to the defendant's interest in the computer or software. If a person used his employer's computer in violation of subsection (a),(b), or (c) he would have no forfeitable interest in it.

Subsection 1028(e) sets out definitions that apply to the section, most of which have been discussed in connection with the other subsections. The key term "computer" means an electronic, magnetic, electrochemical or other high speed data processing device performing logical, arithemetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. It includes home as well as business computers.

"Property", a term used in subsection (a) to describe the object of a computer fraud or theft scheme, is defined to specifically include information and "computer services". In turn "computer services" is defined to include computer time, data processing and data storage facilities. Thus, a person who with criminal intent used a computer to access another computer, a computer system or computer network, and used the other computer, computer system or network to perform calculations or process or store data would be guilty of a violation of subsection 1028(a). Similarly, a person who with criminal intent used a computer to access another computer, computer system, or network in a way that prevented access by legitimate users would also violate subsection 1028(a) because he has taken computer time. These situations are to be contrasted with the simple unauthorized access provisions of 1028(c) which would apply if the accessed computer, system, or network was not used for calculations or storage and if the access did not prevent simultaneous access by a legitimate user.

Section three of the bill amends the table of sections of Chapter 47 of title 18 to reflect the addition of the new section 1028 concerning computer fraud and abuse.