FOIA Number: 2019-0203-F

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

Collection/Record Group: Clinton Presidential Records

Subgroup/Office of Origin: Special Projects

Series/Staff Member: General Files

Subseries:

OA/ID Number: 14132

FolderID:

Folder Title:
[Intellectual Property Rights Working Group]: NII [National Information Infrastructure]

Stack:	Row:	Section:	Shelf:	Position:
S	65	1	1	2

Withdrawal/Redaction Sheet
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. memo	re: Legislative referral memorandum [partial] (1 page)	05/10/1995	P3/b(3)

COLLECTION:
Clinton Presidential Records
Sepcial Projects
General Files
OA/Box Number: 14132

FOLDER TITLE:
[Intellectual Property Rights Working Group]: NII [National Information Infrastructure]

2019-0203-F
jm2862

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. memo	re: Legislative referral memorandum [partial] (1 page)	05/10/1995	P3/b(3)

COLLECTION:
Clinton Presidential Records
Sepcial Projects
General Files
OA/Box Number: 14132

FOLDER TITLE:
[Intellectual Property Rights Working Group]: NII [National Information Infrastructure]

2019-0203-F
jm2862

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
Washington, D.C. 20503-0001

5/3/95

LEGISLATIVE REFERRAL MEMORANDUM

LRM NO: 1183

FILE NO: 806

Total Page(s): ____

TO: Legislative Liaison Officer - See Distribution below:

FROM: James JUKES (for)
Assistant Director for Legislative Reference

OMB CONTACT: Ronald JONES 395-3386
Legislative Assistant's line (for simple responses): 395-3454

SUBJECT: JUSTICE Proposed Draft Bill: National Information Infrastructure Protection Act of 1995

DEADLINE: Wednesday, May 10,1995

In accordance with OMB Circular A-19, OMB requests the views of your agency on the above subject before advising on its relationship to the program of the President.

Please advise us if this item will affect direct spending or receipts for purposes of the "Pay-As-You-Go" provisions of Title XIII of the Omnibus Budget Reconciliation Act of 1990.

COMMENTS:

DISTRIBUTION LIST:

AGENCIES:

(b)(3)

[001]

324-COMMERCE - Michael A. Levitt - (202) 482-3151
325-DEFENSE - Samuel T. Brick, Jr. - (703) 697-1305
207-EDUCATION - John Kristy - (202) 401-8313
260-Federal Communications Commission - Steve Klitzman - (202) 418-1900
237-General Services Administration - William R. Ratchford - (202) 501-0563
328-HHS - Vacant - (202) 690-7760
429-National Economic Council - Sonyia Matthews - (202) 456-2174
249-National Security Council - Andrew D. Sens - (202) 456-9221
288-Office of Science and Technology Policy - Elisa Wynn - (202) 456-6020
291-Securities and Exchange Commission - Kate Fulton - (202) 942-0014
228-TREASURY - Richard S. Carro - (202) 622-1146
SSA
USAS
~~SSA~~

EOP:
Tom Kalil
Mike Nelson
Greg Simon
Chris Cerf
Jose Cerda
Bruce McConnell
Ed Springer
Chris Brown
Jim Duke
Tina Westby-Jonas
Steve Aitken
John Podesta

RESPONSE TO
LEGISLATIVE REFERRAL MEMORANDUM

LRM NO: 1183
FILE NO: 806

If your response to this request for views is simple (e.g., concur/no comment), we prefer that you respond by e-mail or by faxing us this response sheet.

If the response is simple and you prefer to call, please call the branch-wide line shown below (NOT the analyst's line) to leave a message with a legislative assistant.

You may also respond by:

(1) calling the analyst/attorney's direct line (you will be connected to voice mail if the analyst does not answer); or
(2) sending us a memo or letter.

Please include the LRM number shown above, and the subject shown below.

TO: Ronald JONES 395-3386
Office of Management and Budget
Fax Number: 395-3109
Branch-Wide Line (to reach legislative assistant): 395-3454

FROM: _____ (Date)

_____ (Name)

_____ (Agency)

_____ (Telephone)

SUBJECT: JUSTICE Proposed Draft Bill: National Information Infrastructure Protection Act of 1995

The following is the response of our agency to your request for views on the above-captioned subject:

_____ Concur

_____ No Objection

_____ No Comment

_____ See proposed edits on pages _____

_____ Other: _____

_____ FAX RETURN of ____ pages, attached to this response sheet

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 1, 1995

Honorable Alice M. Rivlin
Director
Office of Management and Budget
Washington, D. C. 20503

Dear Ms. Rivlin:

Enclosed are copies of a proposed communication to be transmitted to the Congress relative to: a draft legislative proposal entitled the "National Information Infrastructure Protection Act of 1995."

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

Sincerely,

Kent Markus
Acting Assistant Attorney General

Enclosure

*To coordinate clearance contact: Velma Taylor, 514-7279.

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

Honorable Newt Gingrich
Speaker
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Speaker:

Enclosed for your consideration is proposed legislation titled the "National Information Infrastructure Protection Act of 1995." The proposed amendments would provide enhanced protection for the National Information Infrastructure (NII) by strengthening existing criminal provisions covering conduct that threatens computers and the valuable information they contain.

The proposed legislation addresses gaps in the statutory scheme under 18 U.S.C. § 1030, the principal Federal computer crime statute. Since this law was first enacted in 1984, we have gained considerable experience in applying its subsections to various forms of computer crime. As technologies have advanced and become increasingly important to our society, particularly with respect to government, commerce, science, medicine, and education, we have come to realize that the statutory scheme in its current form does not adequately address all forms of conduct that may be harmful to the Federal government's interests in protecting computers and information. Consequently, we propose several measures designed to close loopholes and otherwise enhance the provisions of section 1030.

Specifically, the proposed legislation would tighten the prohibition on gaining unauthorized access to national security information from a computer by making it a crime to obtain such information if the information could be used against the national interest, rather than requiring knowledge that the information would be so used. Similarly, in view of many reported instances of persons having gained unauthorized access to other government data in computers, such as information on criminal histories in National Crime Information Center computers and draft court opinions in judges' computers, the legislation would make it a crime to get unauthorized computer access to such data. Along the same lines, the amendments would make it clear that any unauthorized access to a government computer or the data it contains is illegal. The proposal also would enhance the anti-

fraud features of the statute by making it illegal to access a computer without or in excess of authority when significant computer time is obtained.

The most substantial revisions to section 1030 involve a complete reworking of section 1030(a)(5), the provision governing damaging intrusions into computers by "hackers." Most notably, when the statute was amended in 1994, certain government and financial institution computers may have been denied previously existing Federal protection, some hacking activities may have been inappropriately decriminalized, and certain insider conduct may have been inappropriately criminalized. We have therefore revisited this provision in some detail.

Finally, we have added a provision covering extortion directed against computer systems, amended the definition of "Federal interest computer" to recognize the global reach of existing networks, and made a few more minor adjustments to fine-tune the statute in light of the proposed substantive revisions.

In drafting the proposed legislation, we have carefully considered what amendments are most immediately necessary to address increasing concerns that we protect the valuable information that is becoming available through the NII and through computers in all segments of modern society. We believe the provisions proposed here represent the best possible approach to affording that protection, while recognizing the need to avoid heavy-handed or draconian measures in regulating access to information and computers.

The Office of Management and Budget has advised that there is no objection from the standpoint of the Administration's program to the presentation of this legislative proposal to the Congress.

Sincerely,

Kent Markus
Acting Assistant Attorney General

Enclosure

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

Honorable Albert Gore, Jr.
President
U.S. Senate
Washington, D.C. 20510

Dear Mr. President:

Enclosed for your consideration is proposed legislation titled the "National Information Infrastructure Protection Act of 1995." The proposed amendments would provide enhanced protection for the National Information Infrastructure (NII) by strengthening existing criminal provisions covering conduct that threatens computers and the valuable information they contain.

The proposed legislation addresses gaps in the statutory scheme under 18 U.S.C. § 1030, the principal Federal computer crime statute. Since this law was first enacted in 1984, we have gained considerable experience in applying its subsections to various forms of computer crime. As technologies have advanced and become increasingly important to our society, particularly with respect to government, commerce, science, medicine, and education, we have come to realize that the statutory scheme in its current form does not adequately address all forms of conduct that may be harmful to the Federal government's interests in protecting computers and information. Consequently, we propose several measures designed to close loopholes and otherwise enhance the provisions of section 1030.

Specifically, the proposed legislation would tighten the prohibition on gaining unauthorized access to national security information from a computer by making it a crime to obtain such information if the information could be used against the national interest, rather than requiring knowledge that the information would be so used. Similarly, in view of many reported instances of persons having gained unauthorized access to other government data in computers, such as information on criminal histories in National Crime Information Center computers and draft court opinions in judges' computers, the legislation would make it a crime to get unauthorized computer access to such data. Along the same lines, the amendments would make it clear that any unauthorized access to a government computer or the data it contains is illegal. The proposal also would enhance the anti-fraud features of the statute by making it illegal to access a

computer without or in excess of authority when significant computer time is obtained.

The most substantial revisions to section 1030 involve a complete reworking of section 1030(a)(5), the provision governing damaging intrusions into computers by "hackers." Most notably, when the statute was amended in 1994, certain government and financial institution computers may have been denied previously existing Federal protection, some hacking activities may have been inappropriately decriminalized, and certain insider conduct may have been inappropriately criminalized. We have therefore revisited this provision in some detail.

Finally, we have added a provision covering extortion directed against computer systems, amended the definition of "Federal interest computer" to recognize the global reach of existing networks, and made a few more minor adjustments to fine-tune the statute in light of the proposed substantive revisions.

In drafting the proposed legislation, we have carefully considered what amendments are most immediately necessary to address increasing concerns that we protect the valuable information that is becoming available through the NII and through computers in all segments of modern society. We believe the provisions proposed here represent the best possible approach to affording that protection, while recognizing the need to avoid heavy-handed or draconian measures in regulating access to information and computers.

The Office of Management and Budget has advised that there is no objection from the standpoint of the Administration's program to the presentation of this legislative proposal to the Congress.

Sincerely,

Kent Markus
Acting Assistant Attorney General

Enclosure

A BILL

Be it enacted by the Senate and House of Representatives of the United States in Congress assembled, that this Act may be cited as the "National Information Infrastructure (NII) Protection Act of 1995."

Sec. 001. Computer Crime

Section 1030 of title 18, United States Code, is amended --

(1) in paragraph (a)(1) --

(i) by striking "the intent or"; and

(ii) by striking "is to be used" and inserting "could be used";

(2) in paragraph (a)(2) --

(i) by inserting a colon after "obtains" and redesignating the remainder as a new subparagraph (A); and

(ii) by adding at the end the following new subparagraphs:

"(B) information from any department or agency of the United States; or

"(C) information from any Federal interest computer if the conduct involved an interstate or foreign communication;";

(3) in paragraph (a)(3) --

(i) by striking "adversely"; and

(ii) by striking "the use of the Government's operation of such computer" and inserting "that use";

(4) in paragraph (a)(4) by inserting "and the value of such use is $5,000 or less in any one-year period" after "use of the computer";

(5) by amending paragraph (a)(5) to read as follows:

"(5)(A) knowingly causes the transmission of a program, information, code or command and, as a result of such conduct, intentionally causes damage, without authorization, to a Federal interest computer;

"(B) intentionally accesses a Federal interest computer without authorization and as a result of such conduct recklessly causes damage; or

"(C) intentionally accesses a Federal interest computer without authorization and as a result of such conduct causes damage;";

(6) in subparagraph (a)(6)(B) by adding "or" at the end thereof;

(7) by adding a new paragraph (a)(7) as follows:

"(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a Federal interest computer;"

(8) in subparagraph (c)(2)(A) by inserting ", (a)(5)(C)," after "(a)(3)";

(9) in subparagraph (c)(2)(B) by redesignating this subparagraph as (C) and inserting a new subparagraph (B) as follows:

"(B) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(2) if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000;";

(10) in subparagraph (c)(3)(A) --

(i) by striking "or" after "(a)(4)" and inserting a comma; and

(ii) by inserting ", (a)(5)(B), or (a)(7)" after "(a)(5)(A)";

(11) in subparagraph (c)(3)(B) --

(i) by striking "or" after "(a)(4)" and inserting a comma; and

(ii) by inserting "(A), (a)(5)(B), or (a)(5)(C)" after "(a)(5)";

(12) in subsection (d) by inserting "subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of" after "investigate offenses under";

(13) in subparagraph (e)(2)(A) by striking "the use of the financial institution's operation or the Government's operation of such computer" and inserting "that use";

(14) in subparagraph (e)(2)(B) by striking "which is one of two or more computers used in committing the offense, not all of which are located in the same State" and inserting "which is used in interstate or foreign commerce or communications";

(15) in paragraph (e)(6) by striking "and" at the end thereof;

(16) in paragraph (e)(7) by striking the period and inserting a semicolon;

(17) in subsection (e) by adding the following two new paragraphs:

"(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information which

"(A) causes loss to one or more others of a value aggregating $1,000 or more during any one-year period;

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals;

"(C) causes physical injury to any person; or

"(D) threatens the public health or safety; and

"(9) the term 'government entity' as used in this subsection includes the Government of the United States, any State or political subdivision thereof, any foreign country, and any state, provincial, municipal or other political subdivision of a foreign country.";

(18) in subsection (g)

(i) by striking ", other than a violation of subsection (a)(5)(B)," and

(ii) by striking "(a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)" and inserting "(a)(5)(A) and (a)(5)(B)";

(19) by striking subsection (h); and

(20) by striking "such subsection" each place it appears and inserting "this section".

§ 1030. Fraud and related activity in connection with computers

(a) Whoever --

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with ~~the intent or~~ reason to believe that such information so obtained ~~is to be used~~ could be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains:

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any Federal interest computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct ~~adversely~~ affects ~~the use of the Government's operation of such computer~~ that use ;

(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access,
and by means of such conduct furthers the intended fraud and obtains
anything of value, unless the object of the fraud and the thing obtained
consists only of the use of the computer and the value of such use is $ 5,000 or less in any one-year period;

~~(5)(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if~~

~~(i) the person causing the transmission intends that such transmission will~~

~~(I) damage, or causes damage to, a computer, computer system, network, information, data, or program; or~~

~~(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program; and~~

~~(ii) the transmission of the harmful component of the program, information, code, or command~~

~~(I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and~~

~~(II)(aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1 year period; or~~

~~(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or~~

~~(B) through means of a computer used in interstate commerce or communication, and knowingly causes the transmission of a program, information, code, or command to a computer or computer system~~

~~(i) with reckless disregard of a substantial and unjustifiable risk that the transmission will~~

~~(I) damage, or cause damage to, a computer, computer system, network, information, data or program; or~~

~~(II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data or program; and~~

~~(ii) if the transmission of the harmful component of the program, information, code, or command~~

~~(I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and~~

~~(II)(aa) causes loss or damage to one or more other persons of a value aggregating $1,000 or more during any 1 year period; or~~

~~(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals;~~

(5)(A) knowingly causes the transmission of a program, information, code or command and, as a result of such conduct, intentionally causes damage, without authorization, to a Federal interest computer;

(B) intentionally accesses a Federal interest computer without authorization and as a result of such conduct recklessly causes damage; or

(C) intentionally accesses a Federal interest computer without authorization and as a result of such conduct causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if --

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; or

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a Federal interest computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is --

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under ~~such subsection~~ this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under ~~such subsection~~ this section, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C) or (a)(6) of this section which does not occur after a conviction for another offense under ~~such subsection~~ this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(2) if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the

Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000;

~~(B)~~ (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under ~~such subsection~~ this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), ~~or~~ (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under ~~such subsection~~ this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), ~~or~~ (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under ~~such subsection~~ this section, or an attempt to commit an offense punishable under this subparagraph; and

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section --

(1) the term "computer" means an electronic, magnetic, optical, 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, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "federal interest computer" means a computer --

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the

offense affects ~~the use of the financial institution's operation or the Government's operation of such computer~~ that use; or

(B) ~~which is one of two or more computers used in committing the offense, not all of which are located in the same State~~ which is used in interstate or foreign commerce or communications;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means --

(A) an institution 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) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the

Farm Credit Act of 1971;

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

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; ~~and~~

(7) the term "department of the United States" means the

legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5~~.~~;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information which

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one-year period;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens the public health or safety; and

(9) the term "government entity" as used in this subsection includes the Government of the United States, any State or political subdivision thereof, any foreign country, and any state, provincial, municipal or other political subdivision of a foreign country.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of the section~~, other than a violation of subsection (a)(5)(B),~~ may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection ~~(a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)~~ (a)(5)(A) and (a)(5)(B) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

~~(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under section 1030(a)(5) of title 18, United States Code.~~

LEGISLATIVE ANALYSIS

I. INTRODUCTION: The Need for Legislative Reform

Although there has never been accurate nationwide reporting of computer crime, it is clear from the reports which do exist and from anecdotal information that computer crime is on the rise. For example, the Computer Emergency and Response Team at Carnegie-Mellon University reports that, since 1991, there has been a 498% increase in the number of computer intrusions, and a 702% rise in the number of sites affected. See CERT Annual Report to ARPA. During 1994, for example, approximately 40,000 Internet computers were attacked in 2,460 incidents. Id. Similarly, the FBI's National Computer Crime Squad has opened over 200 hacker cases since the Squad was created in 1991.

That computer crime is on the rise is perhaps a natural result of introducing computers into American society. In an earlier era, the advent of the automobile opened the way for criminals to target the automobile itself (e.g., auto theft) or use it to facilitate traditional crimes (e.g., the bank robbery getaway vehicle). In addition, law enforcement had to learn to seize vehicles to search them for evidence of some offense unrelated to the vehicle itself (e.g., the box of documents in the trunk). In many of the same ways, computers, too, have proven important to criminal investigations. First, a computer may be the target of the offense. In these cases, the criminal's goal is to steal information from, or cause damage to, a computer, computer system, or computer network. Second, the computer may be a tool of the offense. This occurs when an individual uses a computer to facilitate some traditional offense such as fraud (e.g., a bank teller who once stole money from a cash drawer may now use a computer program to skim money directly from depositors' accounts). Last, computers are sometimes incidental to the offense, but significant to law enforcement because they contain evidence of a crime. Narcotics dealers, for example, may use a personal computer to store records pertaining to drug trafficking instead of relying on old-fashioned ledgers.

The different ways in which criminals can use computers have created a philosophical debate among law enforcement experts. Some argue that computer crime is nothing more than traditional crime committed with new, high-tech devices. Others contend that computer crime cannot be analogized to traditional crime and that combatting it requires both innovative law enforcement techniques and new laws designed to address abuses of emerging technologies. In 1984, Congress adopted the latter view and enacted discrete legislation to address crime in electronic environments. Although certain computer crimes appear simply to be old crimes committed in new ways (e.g., the bank teller who uses a computer program to steal money is still committing bank fraud), some computer offenses find their genesis in our new technologies and must be specifically addressed by statute. For example, the

widespread damage caused by inserting a virus into a global computer network cannot be prosecuted adequately by relying upon common law criminal mischief statutes. Indeed, it is questionable whether Robert Morris, the individual responsible for launching the Morris worm and crippling 6,000 computers around the world, could have been prosecuted had Congress not had the foresight to enact the Computer Fraud and Abuse Act.

Whether classified as "old" or "new," computer crime creates unique problems for law enforcement and a concomitant threat to the public welfare. The two most significant problems stem from (1) the shift from a corporeal to an intangible environment, and (2) commingling; that is, individuals can use a single computer to conduct both legal and criminal activities, and to store both contraband and legally possessed (and perhaps statutorily protected) material.

The shift from a corporeal environment (where items are stored in a tangible form which can be physically carried, such as information written on paper) to an intangible, electronic environment means that computer crimes (and the methods used to investigate them) are no longer subject to traditional rules and constraints. Consider, for example, the way the crimes of theft and criminal mischief have evolved. Before the advent of computer networks, the ability to steal information or damage property was to some extent determined by physical limitations. A burglar could break only so many windows and burglarize only so many homes in a week. During each intrusion, the burglar could carry away only so many items. This does not, of course, make this conduct trivial, but it points out that the amount of property a burglar could steal, or the amount of damage he could cause, had physical limits.

In the information age, of course, these limitations no longer apply. A criminal seeking information stored in a networked computer with dial-in access can acquire that information from virtually anywhere in the world. The quantity of information stolen or the amount of damage caused by malicious programming code may be limited only by the speed of the network and the criminal's computer equipment. Moreover, such conduct can easily occur across state and national borders.

Yet despite this clear shift to a borderless, incorporeal environment and the increased risk that information will be stolen and transported in electronic form, laws leave law enforcement without the tools necessary to respond to this new threat. For example, the statute pertaining to interstate transportation of stolen property, 18 U.S.C. § 2314, speaks of "goods, wares and merchandise," and consequently has been held by at least one court not to apply to intangible property. See United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991). Similarly, the long-familiar extortion statute makes it illegal,

in some cases, to threaten physical violence to property. 18 U.S.C. § 1951(a). Although a threat to fire bomb a building would clearly satisfy this test, a threat to delete files may not.

Commingling (using one computer for both legal and illegal purposes, or for storing both contraband and innocuous materials) is another consequence of electronic environments and it, too, represents a serious problem defying simple solution. The fact is, just as a computer can be relevant to a law enforcement inquiry in different ways (i.e., as target, tool, and repository of evidence), a computer can also serve several entirely legitimate functions. First, it can be a storage device, and in this regard the amount of data computers can store continues to increase dramatically. Second, it can be a communications device. New technologies will present other communicative uses (e.g., video teleconferencing), but computers are already used to send and receive faxes and electronic mail, transfer files, and engage in real-time "chat" sessions. Third, computers can be publishing devices. Individuals not affiliated with the traditional press can now widely disseminate facts, opinions, and ideas using desktop publishing applications.

As a result of its many functions, a single computer can be used to conduct both legal and criminal activities, and/or to store both contraband and legally possessed material. Consider, for example, a now classic and frequent law enforcement dilemma: individuals who distribute child pornography or copyrighted software over computer bulletin board systems (BBSs) may make available for downloading a legitimate newsletter on stamp collecting or may offer an electronic mail service. By seizing the BBS, authorities stop the illegal distribution of contraband but, at the same time, may interfere with the distribution of the newsletter and the delivery of electronic mail. Moreover, some of this mail may be between BBS users who have no connection with the illegal activity. Thus, we must carefully balance law enforcement's need to seize computers with the chilling effect such seizures may have.

II. THE STRUCTURE OF TITLE 18 REFORM

There are two ways, conceptually, to address the growing computer crime problem. The first would be to comb through the entire United States Code, identifying and amending every statute potentially affected by the implementation of new computer and telecommunications technologies. The second would be to focus our substantive amendments on the Computer Fraud and Abuse Act to specifically address new abuses that spring from new technologies.

The proposed legislation adopts the latter approach for a host of reasons:

(1) The United States will, in a single statute, address the core issues driving computer and information security at both domestic and international levels; that is, protecting the confidentiality, integrity, and availability of data and systems. Indeed, these three themes provide the foundation for the Organization for Economic Cooperation and Development's (OECD) recently released Guidelines for the Security of Information Systems. They also serve as the linchpin for emerging domestic works on information privacy. See, e.g., Draft Principles for Providing and Using Personal Information, 60 Fed. Reg. 4362 (January 20, 1995) [hereinafter "Draft Principles"]. By patterning the amended Computer Fraud and Abuse Act on the OECD guidelines, we are at the forefront of rethinking how information technology crimes must be addressed: simultaneously protecting the confidentiality, integrity, and availability of data and systems. And by choosing this path, we may encourage other countries to adopt a similar framework, thus creating a more uniform approach to addressing computer crime in the existing global information infrastructure.

(2) In most cases, a single point of reference--The Computer Fraud and Abuse Act, 18 U.S.C. § 1030--is provided for investigators, prosecutors, and legislators as they attempt to determine whether a particular abuse of new technology is covered under federal criminal law.

(3) As new technologies are introduced and the criminal law requires reconsideration, fine-tuning § 1030 may well be adequate, and it will not be necessary to continually parse through the entire United States Code.

(4) This statutory scheme will give us a better understanding of the scope of the computer crime problem by enabling more reliable statistics to be generated regarding computer abuse. Under current law, computer crimes can be charged under a host of criminal statutes, and this situation will continue if we choose a patchwork approach and amend the various provisions of Title 18 to address new computer crimes. The existence of various computer crime provisions in different parts of Title 18 exacerbates an already obvious problem; i.e., computer crime experts have long admitted that there are no centralized computer crime statistics, not even within the law enforcement community. Indeed, a recent study by the United States Sentencing Commission concluded that there were only 76 cases in which the statute of conviction included 18 U.S.C. § 1030, but conceded that the study may have understated the true number of cases because computer crimes may have been charged under other statutes. United States Sentencing Commission, Computer Fraud Working Group Report, pp. 14-15. By centralizing

computer crimes under one statute, we may better measure existing harms, anticipate trends, and determine the need for further legislative reform. Additionally, amendments to the sentencing scheme of 18 U.S.C. § 1030 (and the Federal Sentencing Guidelines--2F1.1--upon which actual sentences are based), will be more effectively determined.

(5) Last, 18 U.S.C. § 1030(f) specifically provides that certain government officials, if engaging in lawfully authorized investigative, protective, or intelligence activities, are not restricted by § 1030. By amending only 18 U.S.C. § 1030 to address new high-tech offenses, we make clear our intent that this exception applies to any newly defined criminal conduct.

III. Specific Amendments -- Protecting the Confidentiality, Integrity, and Availability of Systems and Information

A. Section 1030(a)(1)

Title 18, Section 1030(a)(1) currently provides that anyone who knowingly accesses a computer without authorization or exceeds authorized access and obtains classified information "with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation" is subject to a fine or imprisonment for not more that ten years (for a first offense). 18 U.S.C. § 1030(a)(1)(emphasis added). This scienter element apparently was included when this subsection was originally drafted because it is contained in 18 U.S.C. § 794(a). Section 794(a), however, provides for life imprisonment, whereas § 1030(a)(1) is only a ten-year felony. Therefore, we determined that the language of § 1030(a)(1) should track the language of 18 U.S.C. § 793(e), which also provides a maximum penalty of ten years' imprisonment for obtaining from any source certain items connected with the national defense.

It should be noted that, although there is considerable overlap between § 793(e) and § 1030(a)(1), the two statutes do not reach exactly the same conduct. Section 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information. In this sense then, it is the use of the computer which is being proscribed, not the unauthorized possession of, access to, or control over the information itself. Existing espionage laws would provide an adequate basis for the prosecution of individuals who attempt to peddle governmental secrets to foreign governments. However, a person who deliberately breaks in to a computer for the purpose of obtaining properly classified information, or attempts to do so, should be subject to criminal prosecution for this conduct.

B. Section 1030(a)(2)

Subsection (a)(2) is, in the truest sense, a provision designed to protect the confidentiality of computer data. As was noted in 1986 by the Senate Judiciary Committee, "[t]he premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions. . . . Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data." S. Rep. No. 99-432 at 6.

With the continued evolution of the National Information Infrastructure (NII), however, we have come to recognize that not only financial records and credit information warrant federal protection. As noted in the commentary to the Draft Principles, "with the NII, the assumption is that large amounts of sensitive information will be on line, and can be accessed, perhaps without authority, by a large number of network users." 59 Fed. Reg. at 27207. Moreover, "the NII will only achieve its full potential if individual privacy is properly protected." Id. We have therefore amended subsection 1030(a)(2) to insure that it is punishable to misuse computers to obtain government information and, where appropriate, information held by the private sector. Moreover, we have restructured the provision so that different paragraphs protect different types of information, thus allowing us to easily add or modify offenses if events require.

We recognize that not all computer misuse warrants federal criminal sanctions. The problem is that no litmus test can accurately segregate important from unimportant information, and any legislation may therefore be under- or over-inclusive. For example, a frequent test for determining the appropriateness of federal jurisdiction--a monetary amount--does not work well when protecting information. The theft from a computer of a judge's draft opinion in a sensitive case, or the copying of medical records, might not meet such a monetary threshold, but clearly such information should be protected and the act of taking it criminalized. It is important to remember that the elements of the offense include not just taking the information, but abusing one's computer authorization to do so.

The need to protect information is highlighted by recent studies indicating that people are increasingly misusing computers to obtain information. In 1993, the General Accounting Office (GAO) presented testimony before the House Government Operations Committee, Subcommittee on Information, Justice, Agriculture, and Transportation, on the abuse of National Crime

Information Center (NCIC) information.[1] The testimony stated that, following an investigation, GAO determined that (1) NCIC information is valuable, (2) such information has been misused by "insiders" (individuals with authorized access), (3) this misuse included selling NCIC information to outsiders and determining whether friends and relatives had criminal records, and (4) incentives for misuse outweighed potential penalties. Statement of Laurie E. Ekstrand, July 28, 1993, p. 6 [hereinafter "Ekstrand Statement"]. The GAO found that some of this misuse jeopardized the safety of citizens and potentially jeopardized law enforcement personnel. Id. at 16. Moreover, because there were no federal or state laws specifically directed at NCIC misuse, most abusers of NCIC were not criminally prosecuted. Id. at 17. GAO concluded that Congress should enact legislation with strong criminal sanctions specifically directed at the misuse of NCIC. Id. at 20.

Of course, protecting solely NCIC data (or, more broadly, criminal history information), would be underinclusive, because other types of sensitive data are clearly at risk. For example, during Operation Desert Storm, it was widely reported that hackers accessed sensitive but unclassified data regarding personnel performance reports, weapons development information, and descriptions of the movements of equipment and personnel. Teen tapped computers of U.S. military, Chicago Tribune, November 21, 1991 at 3. NASA computers have also been penetrated, Computer Hacker Charged with Entering NASA System, Washington Post, September 26, 1991 at A20, as have at least two federal courthouse computer systems. See, e.g., U.S. Says Hackers Scanned Data, The New York Times, November 15, 1992, at A40. Some Internal Revenue Service employees also improperly used IRS computers to examine tax return information. I.R.S. Staff Is Cited in Snoopings, The New York Times, July 19, 1994, at D1, D5.

Clearly, the government should be able to prosecute individuals who obtain government information by misusing computers.[2] Importantly, 18 U.S.C. § 1030(a)(2) does not punish

---

[1] NCIC is currently the nation's most extensive computerized criminal justice information system. It contains criminal history information, files on wanted persons, and information on stolen vehicles and missing persons.

[2] We recognize that 18 U.S.C. § 641 might apply to the theft of government data through computer misuse. At common law, however, theft statutes often required the asportation of the property and, in computer cases, the original information is not moved but rather left in the possession of the victim. Prosecutors have therefore been reluctant to charge individuals with violating § 641 when the stolen property consists of computerized information. See, e.g., Ekstrand Statement at 17-

the mere acquisition of information (which might unduly impede the free flow of ideas), but prohibits intentionally accessing a computer without or in excess of authority and then obtaining such information. Moreover, to the extent that the information obtained is or should be available, it should be obtained through legal means (e.g., public sources, FOIA) and not through hacking.

Subsection 1030(a)(2)(C) is designed to protect against the interstate or foreign theft of information by computer. Such a provision is necessary in light of the Tenth Circuit's decision in United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991), where the court held that purely intangible intellectual property, such as a computer program, cannot constitute goods, wares, merchandise, securities, or moneys which have been stolen, converted, or taken within the meaning of § 2314. "Information" as used in this subsection is to be broadly construed and includes information stored in intangible form. Moreover, consistent with our prior construction of § 1030(a)(2), "obtaining information" includes merely reading it; i.e., there is no requirement that the information be copied or transported. This is critically important because, in an electronic environment, information can be "stolen" without asportation, and the original usually remains intact.

We note that some computers may qualify under more than one subsection of § 1030(a)(2); for example, a particular government computer might be covered by both § 1030(a)(2)(B) and (a)(2)(C). This overlap serves to eliminate legal issues that may arise if the provisions were mutually exclusive. Conceivably, in a given case, it may not be clear whether information taken from a government contractor's computer constitutes "information from any department or agency of the United States" under § 1030(a)(2)(B), but the offense might still be chargeable under § 1030(a)(2)(C) if the elements of that subsection are satisfied.

The seriousness of a breach in confidentiality depends, in considerable part, on the value of the information taken, or on what is planned for the information after it is obtained. Thus, we have structured the statutory penalties to provide that obtaining information of minimal value is only a misdemeanor, but obtaining valuable information, or misusing such information in other more serious ways, is a felony.

More specifically, the crime becomes a felony if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the

---

19. Although there may be some overlap between § 1030(a)(2) and § 641, we do not mean for the former to preempt the latter.

United States or of any State, or if the value of the information obtained exceeds $5,000.

As for non-monetary enhancements, recent documented cases indicate that individuals misuse information for a variety of unacceptable purposes. The terms "for purposes of commercial advantage or private financial gain" and "for the purpose of committing any criminal or tortious act" are taken from the copyright statute (17 U.S.C. § 506(a)) and wiretap statute (18 U.S.C. § 2511(1)(d)) respectively, and are intended to have the same meanings as in those statutes.

As for the monetary threshold, any reasonable method can be used to establish the value of the information obtained. For example, the research, development, and manufacturing costs, or the value of the property "in the thieves' market," can be used to meet the $5,000 valuation. See, e.g., United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988).

The relationship between the existing § 1030(a)(3) provision and the newly amended § 1030(a)(2) merits some discussion. Section 1030(a)(3) protects the computer from outsiders, even if the hacker obtains no information. Thus, an intruder who penetrates a government machine to gain network access is nonetheless liable for trespass even when he has not jeopardized the confidentiality of data. Section 1030(a)(2), on the other hand, protects the confidentiality of data, even from intentional misuse by insiders. Additionally, although a first violation of § 1030(a)(3) is always a misdemeanor, a § 1030(a)(2) violation may constitute a felony if the information taken is valuable or sufficiently misused. See § 1030(c)(2)(B)(raising the offense to felony level based upon the value or intended use of the improperly acquired data). Although a single act may violate both provisions, the provisions protect against different harms and, in any event, the actor's conduct would be aggregated for the purposes of sentencing.

C. Subsection 1030(a)(3)

Two substantive changes are proposed to § 1030(a)(3). First, the word "adversely" would be deleted because including this term suggests, inappropriately, that trespassing in a government computer may be benign. Second, for clarity, we would replace the term "the use of the Government's operation of such computer" with the term "that use." When a computer is used for the government, the government is not necessarily the operator, and the old term may lead to confusion. Consistent with this change, a similar change would be made to the definition of federal interest computer in § 1030(e)(2)(A).

D. Subsection 1030(a)(4)

Subsection 1030(a)(4) would be amended to insure that felony level sanctions apply when unauthorized use of the computer (or use exceeding authorization) is significant. At the time the "computer use" exception was crafted, the Senate Judiciary Committee noted that:

> [T]he mere use of a computer or computer service has a value all its own. Mere trespasses onto someone else's computer system can cost the system provider a "port" or access channel that he might otherwise be making available for a fee to an authorized user. At the same time, the Committee believes it is important to distinguish clearly between acts of fraud under (a)(4), punishable as felonies, and acts of simple trespass, punishable in the first instance as misdemeanors. That distinction would be wiped out were the Committee to treat every trespass as an attempt to defraud a service provider of computer time.

S. Rep. No. 99-432, 99th Cong., 2d Sess. 10 (1986). See also H.R. Rep. No. 99-612, 99th Cong., 2d Sess. 12 (1986).

Although we continue to share the concern about converting every trespass into a felony scheme to defraud, we have come to recognize that a blanket exception for computer use may be too broad. Hackers, for example, have broken into Cray supercomputers for the purpose of running password cracking programs, sometimes amassing computer time worth far in excess of $5,000. In light of the large expense to the victim caused by some of these trespassing incidents, it is more appropriate to restrict the exception to cases involving less than $5,000 during any one-year period.

E. Subsection 1030(a)(5)

Subsection 1030(a)(5) was amended in 1994. However, the 1994 law may have some unintended consequences. Most notably, certain government and financial institution computers may have been denied previously existing federal protection; some hacking activities may have been inappropriately decriminalized; and certain insider conduct may have been inappropriately criminalized. We have therefore revisited this provision.

In 1994, the reach of this subsection was broadened by replacing the term "federal interest computer" with the term "computer used in interstate commerce or communications." The latter term is broader because the definition of federal interest

computer in 18 U.S.C. § 1030(e)(2)(B) covered a computer "which is one of two or more computers used in committing the offense, not all of which are located in the same State." This meant that hackers who attacked other computers in their own state were not subject to federal jurisdiction, notwithstanding the fact that their actions may have severely affected interstate or foreign commerce. For example, individuals who attack telephone switches may disrupt interstate and foreign calls. The 1994 change remedied that defect.

The definition of federal interest computer, however, actually covered more than simply interstate activity. More specifically, 18 U.S.C. § 1030(e)(2)(A) covered, generically, computers belonging to the United States Government or financial institutions, or those used by such entities on a non-exclusive basis if the conduct constituting the offense affected the Government's operation or the financial institution's operation of such computer. By changing § 1030(a)(5) from "federal interest computer" to "computer used in interstate commerce or communications," Congress may have inadvertently eliminated federal protection for those government and financial institution computers not used in interstate communications. For example, the integrity and availability of classified information contained in an intrastate local area network may not have been protected under the 1994 version of 18 U.S.C. § 1030(a)(5), although its confidentiality continued to be protected under 18 U.S.C. § 1030(a)(1). To remedy this situation, we have proposed to reinsert the term "federal interest computer" in § 1030(a)(5) and to amend the definition in § 1030(e)(2)(B), to address our original concerns regarding intrastate "phone phreakers" (i.e., hackers who penetrate telecommunications computers).

We have also defined "federal interest computer" specifically to include those computers used in "foreign" communications. With the continually expanding global information infrastructure, with numerous instances of international hacking, and with the growing possibility of increased global industrial espionage, it is important that the United States have jurisdiction over international computer crime cases. Arguably, the old definition contained in 18 U.S.C. § 1030(e)(2) conferred such jurisdiction because the requirement that the computers used in committing the offense not all be located in the same state might be satisfied if one computer were located overseas. As a general rule, however, Congress' laws have been presumed to be domestic is scope only, absent a specific grant of extraterritorial jurisdiction. E.E.O.C. v. Arabian American Oil Co., 499 U.S. 244 (1991). To insure that our intent is clear, the statute would be amended to reference international communications.

Another concern with the 1994 version of 18 U.S.C. § 1030(a)(5) involves the overall statutory scheme. Under the 1986 version of subsection 1030(a)(5), the actor causing the harm must have been without authority to access the victim computer. As such, the provision did not apply to insiders, although insiders are often responsible for intentionally causing computer damage. Indeed, the Justice Department was forced to decline prosecution in some cases where individuals intentionally inserted malicious programming code into computers, because those individuals were authorized to access the attacked system. The 1994 law, in contrast to the 1986 version, appropriately applies to both insiders and those without authorized access.

Unfortunately, however, by eliminating the trespassing requirement, and at the same time requiring the government to prove that the actor either intentionally or recklessly caused damage, the law no longer punishes a person who broke into a federal interest computer and "thereby caused loss." See 18 U.S.C. § 1030(a)(5)[1986 version]. Thus, the enactment of the 1994 legislation decriminalized some hacking and inadvertently sent the message that breaking into computers was acceptable so long as the actor neither intended nor recklessly caused damage. Criminal liability for such behavior should be restored, in light of the increased importance of computer networks in today's society and the nation's considerable interest in creating a trusted national information infrastructure that insures the confidentiality, integrity, and availability of information and systems.

The problem arose because the 1986 and 1994 versions of section 1030(a)(5) defined improper conduct in different, but nonetheless singular ways--the former by focusing on the actor's authority to access the computer; the latter by considering the actor's intent. These two different litmus tests, of course, cover quite different activity, but neither measure, taken alone, succeeds in describing the acts which should be criminal. For example, although those who intentionally damage a system should be punished regardless of whether they are authorized users, it is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional. In such cases, it is the intentional act of trespass that makes the conduct criminal. To provide otherwise is to openly invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause, it is no crime unless that damage was either intentional or reckless. Rather then send such a dangerous message (and deny victims any relief), it is better to insure that § 1030(a)(5) criminalizes all computer trespass, as well as intentional damage by insiders, albeit at different levels of severity.

By using a matrix, it is easy to see that neither the 1986 law nor the 1994 law was adequate, although they fail in different categories.

MATRIX 1: § 1030(a)(5)[1986 Version]

[Based on the defendant's authority to access the computer]

	Trespassers	**Authorized Users**
Intentional Damage	Felony	No crime
Reckless Damage	Felony	No crime
Negligent Damage	Felony	No crime

MATRIX 2: 18 U.S.C. § 1030(a)(5)[1994 Version]

[Based on the defendant's criminal intent to damage]

	Trespassers	**Authorized Users**
Intentional Damage	Felony	Felony
Reckless Damage	Misdemeanor	Misdemeanor
Negligent Damage	No crime	No crime

Conceptually, a comprehensive statutory scheme would not treat these two tests--mental state and authority to access--as mutually exclusive. Instead, it would integrate them to cover all kinds of serious misconduct. Just as important, it would recognize that some behaviors are less serious, or should not be criminal offenses at all. For example, the 1994 law created a misdemeanor for reckless damage without distinguishing between trespassers and authorized users. Whether authorized users should ever be criminally liable for reckless damage is a debatable question. For example, it could be deemed reckless in today's computer environment to intentionally copy a file from a floppy diskette to a hard drive without first running a virus scan--although imposing criminal sanctions for such conduct is clearly inappropriate, absent other evidence of criminal intent. On the other hand, reckless trespassers warrant felony

prosecutions, since they are unauthorized users who pose significant risks to computer systems. Thus, a more sensible approach integrates access and authority tests in the following way:

MATRIX 3: 18 U.S.C. § 1030(a)(5) [THE NEW LAW]

[Based on the defendant's authority to access the computer and criminal intent to damage]

	Trespassers	**Authorized Users**
Intentional Damage	Felony	Felony
Reckless Damage	Felony	No crime
Negligent Damage	Misdemeanor	No crime

Essentially, this matrix provides that individuals who access protected computers without authority are responsible for the consequences of their actions, but those accessing with authority are criminally liable only if they intend to cause damage to the victim. Although subsections § 1030(a)(5)(B) and (a)(5)(C) require that the actor cause damage as a result of his or her unauthorized access, we do not intend that damages be limited to those caused by the process of gaining illegal entry. Rather, all damage, whether caused while gaining access or after entry, is relevant.

Another concern with the 1994 law was that it required both "damage" and "loss," without clearly articulating what constituted "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information was damaged. Nonetheless, the intruder's conduct allows him to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to re-securing the system. Thus, although there is arguably no "damage," the victim does suffer "loss." In our view, if the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.

It was not possible to address all of these concerns by making only minor amendments to subsection 1030(a)(5). Thus, we altered the statutory scheme to both simplify its provisions and adopt the sanctions provided in Matrix 3. As discussed further below, we retained the term "damage," but have now provided a definition of that term in 18 U.S.C. § 1030(e)(8). Consistent with our view that § 1030(a)(5) protects the integrity and availability of data and systems, "damage" means any impairment of those attributes. We have deliberately avoided listing specific acts that can cause such impairment to insure that the statute is suitably broad. For example, in the 1986 version, the terms "alters, damages or destroys information," were included, inadvertently raising new issues (e.g., whether encrypting data satisfies this test since the underlying original information remains unchanged). Rather than providing a list of prohibited actions and risk being underinclusive, we propose to focus instead on the harm we wish to prevent.

The definition of "damage" can now be found in subsections 1030(e)(8)(A) through (D). As in the past, the term "damage" will require either significant financial losses, § 1030(e)(8)(A), or potential impact on medical treatment, § 1030(e)(8)(B). We have suggested also adding two other concerns: causing physical injury to any person, 18 U.S.C. § 1030(e)(8)(c), and threatening the public health or safety, 18 U.S.C. § 1030(e)(8)(c). As the NII and other network infrastructures continue to grow, computers will increasingly be used for access to critical services such as emergency response systems and air traffic control, and will be critical to other systems which we cannot yet anticipate. Thus, we sought to define "damage" broadly to encompass the types of harms against which people should be protected.

Having amended the structure of § 1030(a)(5), it was necessary to amend the civil penalty provision under § 1030(g). The new section provides that victims of computer abuse can maintain a civil action against the violator to obtain compensatory damages, injunctive relief, or other equitable relief. Damages are limited to economic damages, unless the defendant violated § 1030(a)(5)(A) or § 1030(a)(5)(B); that is, unless the actor intentionally caused damage, or recklessly caused damage while trespassing in a computer.

F. Subsection 1030(a)(7)

New subsection (a)(7) is designed to respond to a growing problem: the interstate transmission of threats directed against computers and computer networks. Such threats, if accompanied by an intent to extort, may already be covered in some instances by the Hobbs Act, 18 U.S.C. § 1951, which applies to interference with commerce by extortion. They also may be covered in some

instances by 18 U.S.C. § 875(d), which applies to interstate communication of a threat to injure the property of another. However, under both of these statutes, it is not absolutely clear that "property" includes the operation of a computer, or the data or programs stored in a computer and its peripheral equipment. Moreover, it is not clear that certain actions (such as encrypting someone's data and then demanding money for the key) constitute a threat to injure the property of another. See 18 U.S.C. § 875(d).

Our concerns are not theoretical. In one recent case, for example, an individual threatened to crash a computer system unless he was granted access to the system and given an account. Another case involved an individual who penetrated a city government's computer system and encrypted the data on a hard drive, thus leading the victim to suspect an extortion demand was imminent. (This demand never came, however, and fortunately the victim was able to recover from the incident.) Although the number of such incidents is currently small, the explosion in network access has substantially increased the risk that such conduct will occur, and our nation's increased reliance on computers clearly suggests that such activities, if not deterred, will severely impact upon our ability to use the NII effectively. Moreover, since such extortion and threats will normally involve interstate and foreign communications, it is appropriate that Congress act quickly to address this new problem.

It is worth noting that subsection (a)(7) covers any interstate or international transmission of threats against computers, computer networks, and their data and programs, whether the threat is received by mail, a telephone call, electronic mail, or through a computerized messaging service. The provision is worded broadly to cover threats to interfere in any way with the normal operation of the computer or system in question, such as denying access to authorized users, erasing or corrupting data or programs, or slowing down the operation of the computer or system. The extortion element is modeled after that in existing subsections 875(b) and (d), and should be construed in similar fashion.

G. Sentencing Provisions -- 18 U.S.C. § 1030(c)

The sentencing provisions of § 1030 would be altered to reflect the new statutory scheme and to address an old, technical error. As previously enacted, recidivists were only subject to enhanced penalties if they violated the same subsection twice. For example, if an individual violated the Act by committing fraud by computer [subsection (a)(4)] and later committed another computer crime offense by intentionally destroying medical records [subsection (a)(5)], he was not a recidivist because his conduct violated two separate subsections of § 1030. We have changed the statutory language to provide that anyone who is

convicted twice of committing a computer offense will be subjected to enhanced penalties.

H. Jurisdiction -- 18 U.S.C. § 1030(d)

Having created several new crimes in 18 U.S.C. § 1030, it became necessary to consider the jurisdictional grant in 18 U.S.C. § 1030(d). For some time, the Federal Bureau of Investigation and the United States Secret Service have shared concurrent jurisdiction over § 1030 based upon a Memorandum of Understanding. By creating certain new crimes, we do not mean to alter any existing agreements. Also, we do not intend to limit or alter an agency's "traditional" jurisdiction. Thus, we have added language to 18 U.S.C. § 1030(d) to insure that the status quo is maintained. For example, 18 U.S.C. § 1030(a)(2)(C) is meant to address gaps in 18 U.S.C. § 2314 (interstate transportation of stolen property), and 18 U.S.C. § 1030(a)(7) is meant to address gaps in 18 U.S.C. § 1951 (the Hobbs Act) and 18 U.S.C. § 875 (interstate communications). All of these statutes are within the traditional jurisdiction of the FBI, and 18 U.S.C. § 1030(d) therefore provides that the FBI would retain exclusive jurisdiction over these types of offenses, even if they are committed by computer.

I. Mandatory Reporting -- 18 U.S.C. § 1030(h)

Lastly, we have eliminated the previously enacted reporting requirement under § 1030(a)(5). As we noted at the outset, by insuring that most high-tech crimes can be charged under § 1030, reports regarding § 1030 convictions may provide more meaningful information on the computer crime problem, as least from a law enforcement perspective, than currently exists. If needed, such statistics could be generated at any time, but to create a mandatory, routine reporting requirement seems, upon reflection, to be unnecessary. This is especially true since computer security organizations, such as the Forum of Incident Response and Security Teams (FIRST), are already spearheading a more comprehensive statistical effort addressing not just computer crime, but computer incidents generally.