

Calendar No. 941

106TH CONGRESS
2D SESSION

S. 2448

To enhance the protections of the Internet and the critical infrastructure of the United States, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 13, 2000

Mr. HATCH (for himself, Mr. SCHUMER, Mr. ABRAHAM, and Mr. KYL) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

OCTOBER 5 (legislative day, SEPTEMBER 22), 2000

Reported by Mr. HATCH, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

A BILL

To enhance the protections of the Internet and the critical infrastructure of the United States, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) ~~SHORT TITLE.~~—This Act may be cited as the

5 “Internet Integrity and Critical Infrastructure Protection

6 Act of 2000”.

1 (b) TABLE OF CONTENTS.—The table of contents for
 2 this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—CYBER-HACKING

- Sec. 101. Deterrence and prevention of fraud; abuse; and criminal acts in connection with computers.
- Sec. 102. Criminal and civil forfeiture for computer fraud and abuse.
- Sec. 103. Enhanced coordination of Federal agencies.
- Sec. 104. Deterring juvenile involvement in computer crimes.
- Sec. 105. Additional defense to civil actions relating to preserving records in response to government request.
- Sec. 106. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse.
- Sec. 107. Forfeiture of devices used in computer software counterfeiting and intellectual property theft.
- Sec. 108. Sentencing directives for computer crimes.
- Sec. 109. Assistance to Federal, State, and local computer crime enforcement and establishment of National Cyber-Crime Technical Support Center.

TITLE II—ANTI-FRAUD PROTECTIONS

- Sec. 201. Protection from fraudulent unsolicited electronic mail.

TITLE III—PRIVACY AND CONFIDENTIALITY PROTECTIONS

- Sec. 301. Privacy protection concerning pen registers and trap and trace devices.
- Sec. 302. Privacy protection for subscribers of satellite television services.
- Sec. 303. Encryption reporting requirements.
- Sec. 304. Fraud in online collection and dissemination of personally identifiable information.
- Sec. 305. National media campaign on public awareness regarding online security and privacy.
- Sec. 306. Fraudulent access to personally identifiable information.

TITLE IV—NATIONAL SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

- Sec. 401. Deputy Assistant Attorney General for Computer Crime and Intellectual Property.
- Sec. 402. National Infrastructure Protection Center.
- Sec. 403. Personnel exchange programs for critical infrastructure protection training.

TITLE V—INTERNATIONAL COMPUTER CRIME ENFORCEMENT

- Sec. 501. Short title.
- Sec. 502. Disclosure of computer crime evidence to foreign law enforcement authorities relating to enforcement of foreign computer crime laws.

- Sec. 503. Investigative assistance to foreign law enforcement authorities to obtain computer crime evidence relating to enforcement of foreign computer crime laws.
- Sec. 504. Court orders to provide assistance to foreign law enforcement authorities relating to enforcement of foreign computer crime laws.
- Sec. 505. Limitations on activities under computer crime mutual assistance agreements.
- Sec. 506. Reimbursement.
- Sec. 507. Judicial review.
- Sec. 508. Computer crime mutual assistance agreements.
- Sec. 509. Preservation of existing authority.
- Sec. 510. Report to Congress.
- Sec. 511. Definitions.

TITLE VI—SEVERABILITY

- Sec. 601. Severability.

- 1 **TITLE I—CYBER-HACKING**
- 2 **SEC. 101. DETERRENCE AND PREVENTION OF FRAUD,**
- 3 **ABUSE, AND CRIMINAL ACTS IN CONNECTION**
- 4 **WITH COMPUTERS.**
- 5 (a) **PENALTIES.**—Subsection (c) of section 1030 of
- 6 title 18, United States Code, is amended—
- 7 (1) in paragraph (2)—
- 8 (A) in subparagraph (A)—
- 9 (i) by inserting “except as provided in
- 10 subparagraph (B),” before “a fine”; and
- 11 (ii) by striking “and” at the end;
- 12 (B) in subparagraph (B), by inserting “or
- 13 an attempt to commit an offense punishable
- 14 under this subparagraph,” after “subsection
- 15 (a)(2),” in the matter preceding clause (i); and
- 16 (C) in subparagraph (C), by striking
- 17 “and” at the end;

1 (2) in paragraph (3)—

2 (A) by striking “, (a)(5)(A), (a)(5)(B),”

3 both places it appears; and

4 (B) by striking “and” at the end; and

5 (3) by adding at the end the following new
6 paragraphs:

7 “(4)(A) except as provided in subparagraph
8 (B), a fine under this title, imprisonment for not
9 more than 3 years, or both, in the case of an offense
10 under subsection (a)(5)(A) or (a)(5)(B) which does
11 not occur after a conviction for another offense
12 under this section, or an attempt to commit an of-
13 fense punishable under this subparagraph;

14 “(B) a fine under this title, imprisonment for
15 not more than 10 years, or both, in the case of an
16 offense under subsection (a)(5)(A) or (a)(5)(B), or
17 an attempt to commit an offense punishable under
18 this subparagraph, if—

19 “(i) the defendant used, or attempted to
20 use, a person less than 18 years of age to com-
21 mit the offense; or

22 “(ii) the offense caused (or, in the case of
23 an attempted offense, would, if completed, have
24 caused)—

1 “(I) loss to one or more persons dur-
2 ing any one-year period (including loss re-
3 sulting from a related course of conduct
4 affecting one or more other protected com-
5 puters) aggregating at least \$5,000 in
6 value;

7 “(II) the modification or impairment,
8 or potential modification or impairment, of
9 the medical examination, diagnosis, treat-
10 ment, or care of one or more individuals;

11 “(III) physical injury to any person;

12 “(IV) a threat to public health or
13 safety; or

14 “(V) damage affecting a computer
15 system used by or for a government entity
16 in furtherance of the administration of jus-
17 tice, national defense, or national security;

18 “(C) a fine under this title, imprisonment for
19 not more than 10 years, or both, in the case of an
20 offense under subsection (a)(5)(A) or (a)(5)(B), or
21 an attempt to commit an offense punishable under
22 this subparagraph, that—

23 “(i) would otherwise be punishable under
24 subparagraph (A); and

1 “(ii) occurs after a conviction for another
2 offense under subsection (a)(5)(A) or (a)(5)(B)
3 for which the defendant was punished under
4 subparagraph (A); and

5 “(D) a fine under this title, imprisonment for
6 not more than 20 years, or both, in the case of an
7 offense under subsection (a)(5)(A) or (a)(5)(B), or
8 an attempt to commit an offense punishable under
9 this subparagraph, that—

10 “(i) would otherwise be punishable under
11 subparagraph (B); and

12 “(ii) occurs after a conviction for another
13 offense under subsection (a)(5)(A) or (a)(5)(B)
14 for which the defendant was punished under
15 subparagraph (B); and

16 “(5) in the case of any felony offense under this
17 section, at the discretion of the court, termination of
18 and ineligibility for any financial assistance for post-
19 secondary education that is available under Federal
20 law, which punishment shall be in addition to any
21 other punishment described in this subsection.”.

22 (b) DEFINITIONS.—Subsection (c) of that section is
23 amended—

1 (1) in paragraph (2)(B), by inserting “, includ-
2 ing a computer located outside the United States”
3 before the semicolon;

4 (2) in paragraph (7), by striking “and” at the
5 end;

6 (3) by striking paragraph (8) and inserting the
7 following new paragraph (8):

8 “(8) the term ‘damage’ means any impairment
9 to the integrity or availability of data, a program, a
10 system, or information;”;

11 (4) in paragraph (9), by striking the period at
12 the end and inserting a semicolon; and

13 (5) by adding at the end the following new
14 paragraphs:

15 “(10) the term ‘conviction’ shall include an ad-
16 judication of juvenile delinquency for a violation of
17 this section;

18 “(11) the term ‘loss’ means any reasonable cost
19 to any victim, including the cost of responding to an
20 offense, conducting a damage assessment, and re-
21 storing the data, program, system, or information to
22 its condition prior to the offense, and any revenue
23 lost, cost incurred, or other consequential damages
24 incurred because of interruption of service;

1 “(12) the term ‘person’ means any person,
2 firm, educational institution, financial institution,
3 government entity, or other entity;”.

4 (c) DAMAGES IN CIVIL ACTIONS.—Subsection (g) of
5 that section is amended in the second sentence by striking
6 “involving damage” and all that follows through the end
7 and inserting “of subsection (a)(5) shall be limited to loss
8 unless such action includes one of the elements set forth
9 in subclauses (II) through (V) of section (e)(4)(B)(ii).”.

10 (d) CERTIFICATION.—That section is further
11 amended—

12 (1) by redesignating subsection (h) as sub-
13 section (i); and

14 (2) by inserting after subsection (g) the fol-
15 lowing new subsection (h):

16 “(h)(1) An offense, or an attempt to commit an of-
17 fense, under subsection (a)(5)(A), (a)(5)(B), or (a)(5)(C)
18 shall not be proceeded against under this section unless—

19 “(A) the offense is punishable under subsection
20 (e)(4)(B); or

21 “(B) the United States Attorney certifies to the
22 appropriate district court of the United States that
23 there is a substantial Federal interest in the offense
24 that warrants the exercise of Federal jurisdiction
25 over the offense.

1 “(2) A certification under paragraph (1)(B) shall not
2 be reviewable by any court.

3 “(3) The Attorney General shall submit to Congress
4 on an annual basis a report on the number of prosecutions
5 undertaken under paragraph (1)(B) during the year pre-
6 ceeding the year in which such report is submitted.”.

7 **SEC. 102. CRIMINAL AND CIVIL FORFEITURE FOR COM-**
8 **PUTER FRAUD AND ABUSE.**

9 (a) **CRIMINAL FORFEITURE.**—Section 1030 of title
10 18, United States Code, as amended by section 101 of this
11 Act, is further amended—

12 (1) by redesignating subsection (h) as sub-
13 section (i); and

14 (2) by inserting after subsection (g) the fol-
15 lowing new subsection (h):

16 “(h)(1) The court, in imposing sentence on any per-
17 son convicted of a violation of this section, shall order,
18 in addition to any other sentence imposed and irrespective
19 of any provision of State law, that such person forfeit to
20 the United States—

21 “(A) the interest of such person in any prop-
22 erty, whether real or personal, that was used or in-
23 tended to be used to commit or to facilitate the com-
24 mission of such violation; and

1 “(B) any property, whether real or personal,
2 constituting or derived from any proceeds that such
3 person obtained, whether directly or indirectly, as a
4 result of such violation.

5 “(2) The criminal forfeiture of property under this
6 subsection, any seizure and disposition thereof, and any
7 administrative or judicial proceeding relating thereto, shall
8 be governed by the provisions of section 413 of the Com-
9 prehensive Drug Abuse Prevention and Control Act of
10 1970 (21 U.S.C. 853), except subsection (d) of that sec-
11 tion.”.

12 (b) CIVIL FORFEITURE.—That section, as amended
13 by subsection (a) of this section, is further amended by
14 inserting after subsection (h) the following new subsection
15 (i):

16 “(i)(1) The following shall be subject to forfeiture to
17 the United States, and no property right shall exist in
18 them:

19 “(A) Any property, whether real or personal,
20 that is used or intended to be used to commit or to
21 facilitate the commission of any violation of this sec-
22 tion.

23 “(B) Any property, whether real or personal,
24 that constitutes or is derived from proceeds trace-
25 able to any violation of this section.

1 “(2) The provisions of chapter 46 of this title relating
2 to civil forfeiture shall apply to any seizure or civil for-
3 feiture under this subsection.”.

4 **SEC. 103. ENHANCED COORDINATION OF FEDERAL AGEN-**
5 **CIES.**

6 Section 1030(d) of title 18, United States Code, is
7 amended—

- 8 (1) by striking “subsections (a)(2)(A),
9 (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of”; and
10 (2) by striking “which shall be entered into by”
11 and inserting “between”.

12 **SEC. 104. DETERRING JUVENILE INVOLVEMENT IN COM-**
13 **PUTER CRIMES.**

14 Section 5032 of title 18, United States Code, is
15 amended in clause (3) of the first undesignated
16 paragraph—

- 17 (1) by striking “or section 1002(a)” and insert-
18 ing “section 1002(a)”; and
19 (2) by inserting after “of this title,” the fol-
20 lowing: “section 1030(a)(1), (a)(2)(B), (a)(3),
21 (a)(5)(A)(i), or (a)(5)(A)(ii) of this title.”.

1 **SEC. 105. ADDITIONAL DEFENSE TO CIVIL ACTIONS RELAT-**
2 **ING TO PRESERVING RECORDS IN RESPONSE**
3 **TO GOVERNMENT REQUEST.**

4 Section 2707(e) of title 18, United States Code, is
5 amended—

6 (1) by redesignating paragraphs (2) and (3) as
7 paragraphs (3) and (4), respectively; and

8 (2) by inserting after paragraph (1) the fol-
9 lowing new paragraph (2):

10 “(2) a request of a governmental entity under
11 section 2703(f) of this title;”.

12 **SEC. 106. AUTHORITY TO INTERCEPT WIRE, ORAL, AND**
13 **ELECTRONIC COMMUNICATIONS RELATING**
14 **TO COMPUTER FRAUD AND ABUSE.**

15 Section 2516(1)(c) of title 18, United States Code,
16 is amended by striking “and section 1341 (relating to mail
17 fraud),” and inserting “section 1341 (relating to mail
18 fraud); a felony violation of section 1030 (relating to com-
19 puter fraud and abuse);”.

20 **SEC. 107. FORFEITURE OF DEVICES USED IN COMPUTER**
21 **SOFTWARE COUNTERFEITING AND INTEL-**
22 **LECTUAL PROPERTY THEFT.**

23 (a) **IN GENERAL.**—Section 2318(d) of title 18,
24 United States Code, is amended—

25 (1) by inserting “(1)” before “When”;

1 appropriate, shall promulgate guidelines or policy statements
2 or amend existing policy statements to address—

3 (1) the potential and actual loss resulting from
4 an offense under section 1030 of title 18, United
5 States Code (as amended by section 101 of this
6 Act);

7 (2) the level of sophistication and planning in-
8 volved in such an offense;

9 (3) the growing incidence of offenses under
10 such subsections and the need to provide an effective
11 deterrent against such offenses;

12 (4) whether or not such an offense was com-
13 mitted for purposes of commercial advantage or pri-
14 vate financial benefit;

15 (5) whether or not the defendant involved a ju-
16 venile in the commission of such an offense;

17 (6) whether or not the defendant acted with
18 malicious intent to cause harm in committing such
19 an offense;

20 (7) the extent to which such an offense violated
21 the privacy rights of individuals harmed by the of-
22 fense; and

23 (8) any other factor the Commission considers
24 appropriate in connection with any amendments
25 made by this Act with regard to such subsections.

1 (b) AMENDMENT OF SENTENCING GUIDELINES RE-
2 LATING TO CERTAIN COMPUTER FRAUD AND ABUSE.—
3 Pursuant to its authority under section 994(p) of title 28,
4 United States Code, the United States Sentencing Com-
5 mission shall amend the Federal sentencing guidelines to
6 ensure that any individual convicted of a violation of sec-
7 tion 1030(a)(5)(A)(iii), of title 18, United States Code (as
8 so amended), can be subjected to appropriate penalties,
9 without regard to any mandatory minimum term of im-
10 prisonment.

11 (c) AMENDMENT OF SENTENCING GUIDELINES RE-
12 LATING TO USE OF ENCRYPTION.—Pursuant to its au-
13 thority under section 994(p) of title 28, United States
14 Code, the United States Sentencing Commission shall
15 amend the Federal sentencing guidelines and, if appro-
16 priate, shall promulgate guidelines or policy statements or
17 amend existing policy statements to ensure that the guide-
18 lines provide sufficiently stringent penalties to deter and
19 punish persons who intentionally use encryption in connec-
20 tion with the commission or concealment of criminal acts
21 sentenced under the guidelines.

22 (d) EMERGENCY AUTHORITY.—The Commission may
23 promulgate the guidelines or amendments provided for
24 under this section in accordance with the procedures set

1 forth in section 21(a) of the Sentencing Act of 1987, as
2 though the authority under that Act had not expired.

3 **SEC. 109. ASSISTANCE TO FEDERAL, STATE, AND LOCAL**
4 **COMPUTER CRIME ENFORCEMENT AND ES-**
5 **TABLISHMENT OF NATIONAL CYBER-CRIME**
6 **TECHNICAL SUPPORT CENTER.**

7 (a) NATIONAL CYBER-CRIME TECHNICAL SUPPORT
8 CENTER.—

9 (1) CONSTRUCTION REQUIRED.—The Director
10 of the Federal Bureau of Investigation shall provide
11 for the construction and equipping of the technical
12 support center of the Federal Bureau of Investiga-
13 tion referred to in section 811(a)(1)(A) of the
14 Antiterrorism and Effective Death Penalty Act of
15 1996 (Public Law 104-132; 110 Stat. 1312; 28
16 U.S.C. 531 note).

17 (2) NAMING.—The technical support center
18 constructed and equipped under paragraph (1) shall
19 be known as the “National Cyber-Crime Technical
20 Support Center”.

21 (3) FUNCTIONS.—In addition to any other au-
22 thorized functions, the functions of the National
23 Cyber-Crime Technical Support Center shall be—

24 (A) to serve as a centralized technical re-
25 source for Federal, State, and local law enforce-

1 ment and to provide technical assistance in the
2 investigations of computer-related criminal ac-
3 tivities;

4 (B) to assist Federal, State, and local law
5 enforcement in enforcing Federal, State, and
6 local criminal laws relating to computer-related
7 crime;

8 (C) to provide training and education for
9 Federal, State, and local law enforcement per-
10 sonnel regarding investigative techniques and
11 forensic analyses pertaining to computer-related
12 crime;

13 (D) to conduct research and to develop
14 technologies for assistance in investigations and
15 forensic analyses of evidence related to com-
16 puter-related crimes;

17 (E) to facilitate and promote efficiencies in
18 the sharing of Federal law enforcement exper-
19 tise and investigative technologies and forensic
20 analysis pertaining to computer-related crimes
21 with State and local law enforcement personnel,
22 prosecutors, regional computer forensic labora-
23 tories and multijurisdictional computer crime
24 task forces; and

1 ~~(F)~~ to carry out such other activities as
2 the Director considers appropriate.

3 ~~(b) DEVELOPMENT AND SUPPORT OF COMPUTER FO-~~
4 ~~RENSIC ACTIVITIES.—~~The Director shall take appropriate
5 actions to develop at least 10 regional computer forensic
6 laboratories, and to provide support, education, and assist-
7 ance for existing computer forensic laboratories, in order
8 that such computer forensic laboratories have the
9 capability—

10 ~~(1)~~ to provide forensic examinations with
11 respect to seized or intercepted computer evi-
12 dence relating to criminal activity;

13 ~~(2)~~ to provide training and education for
14 Federal, State, and local law enforcement per-
15 sonnel and prosecutors regarding investigations,
16 forensic analyses, and prosecutions of com-
17 puter-related crime;

18 ~~(3)~~ to assist Federal, State, and local law
19 enforcement in enforcing Federal, State, and
20 local criminal laws relating to computer-related
21 crime;

22 ~~(4)~~ to facilitate and promote the sharing of
23 Federal law enforcement expertise and informa-
24 tion about the investigation, analysis, and pros-
25 ecution of computer-related crime with State

1 and local law enforcement personnel and pros-
 2 ceutors, including the use of multijurisdictional
 3 task forces; and

4 (5) to carry out such other activities as the
 5 Director considers appropriate.

6 ~~(c) GRANTS TO STATE AND LOCAL LAW ENFORCE-~~
 7 ~~MENT.—~~

8 (1) ~~IN GENERAL.~~—Subject to the provisions of
 9 appropriations Acts, the Assistant Attorney General
 10 for the Office of Justice Programs of the Depart-
 11 ment of Justice shall make a grant to each State,
 12 which shall be used by the State, in conjunction with
 13 units of local government, State and local courts,
 14 other States, or combinations thereof, to establish
 15 and develop programs to—

16 (A) assist State and local law enforcement
 17 agencies in enforcing State and local criminal
 18 laws relating to computer crime;

19 (B) assist State and local law enforcement
 20 agencies in educating the public to prevent and
 21 identify computer crime;

22 (C) educate and train State and local law
 23 enforcement officers and prosecutors to conduct
 24 investigations and forensic analyses of evidence
 25 and prosecutions of computer crime;

1 ~~(D)~~ assist State and local law enforcement
2 officers and prosecutors in acquiring computer
3 and other equipment to conduct investigations
4 and forensic analysis of evidence of computer
5 crimes; and

6 ~~(E)~~ facilitate and promote efficiencies in
7 the sharing of Federal law enforcement exper-
8 tise and information about the investigation,
9 analysis, and prosecution of computer crimes
10 with State and local law enforcement officers
11 and prosecutors, including the use of multijuris-
12 dictional task forces.

13 ~~(2)~~ ASSURANCES.—To be eligible to receive a
14 grant under this subsection, a State shall provide as-
15 surances to the Attorney General that the State—

16 ~~(A)~~ has in effect laws that penalize com-
17 puter crime, such as penal laws prohibiting—

18 ~~(i)~~ fraudulent schemes executed by
19 means of a computer system or network;

20 ~~(ii)~~ the unlawful damaging, destroy-
21 ing, altering, deleting, removing of com-
22 puter software, or data contained in a
23 computer, computer system, computer pro-
24 gram, or computer network; or

1 (iii) the unlawful interference with the
2 operation of or denial of access to a com-
3 puter, computer program, computer sys-
4 tem, or computer network;

5 (B) an assessment of the State and local
6 resource needs, including criminal justice re-
7 sources being devoted to the investigation and
8 enforcement of computer crime laws; and

9 (C) a plan for coordinating the programs
10 funded under this subsection with other Feder-
11 ally funded technical assistant and training pro-
12 grams, including directly funded local programs
13 such as the Local Law Enforcement Block
14 Grant program (described under the heading
15 “Violent Crime Reduction Programs, State and
16 Local Law Enforcement Assistance” of the De-
17 partments of Commerce, Justice, and State, the
18 Judiciary, and Related Agencies Appropriations
19 Act, 1998 (Public Law 105–119)).

20 (3) MATCHING FUNDS.—The Federal share of a
21 grant received under this subsection may not exceed
22 90 percent of the total cost of a program or proposal
23 funded under this subsection unless the Attorney
24 General waives, wholly or in part, the requirements
25 of this paragraph.

1 (4) GRANTS TO INDIAN TRIBES.—Notwith-
2 standing any other provision of this subsection, the
3 Attorney General may use amounts made available
4 under this subsection to make grants to Indian
5 tribes for use in accordance with this subsection.

6 (5) FUNDING.—

7 (A) IN GENERAL.—Of the amount author-
8 ized to be appropriated by subsection (d),
9 \$25,000,000 shall be available for grants under
10 this subsection.

11 (B) LIMITATIONS.—Of the amount made
12 available under subparagraph (A) to carry out
13 this subsection not more than 3 percent may be
14 used by the Attorney General for salaries and
15 administrative expenses.

16 (C) MINIMUM AMOUNT.—Unless all eligible
17 applications submitted by any State or units of
18 local government within a State for a grant
19 under this subsection have been funded, the
20 State, together with grantees within the State
21 (other than Indian tribes), shall be allocated not
22 less than 0.75 percent of the total amount
23 made available under subparagraph (A) for
24 grants pursuant to this subsection, except that
25 the United States Virgin Islands, American

1 Samoa, Guam, and the Northern Mariana Is-
 2 lands each shall be allocated 0.25 percent.

3 (d) AUTHORIZATION OF APPROPRIATIONS.—

4 (1) AUTHORIZATION.—There is hereby author-
 5 ized to be appropriated for fiscal year 2001,
 6 \$125,000,000 for purposes of carrying out this sec-
 7 tion, of which \$20,000,000 shall be available solely
 8 for activities under subsection (b) and of which
 9 \$25,000,000 shall be available solely for activities
 10 under subsection (c).

11 (2) AVAILABILITY.—Amounts appropriated pur-
 12 suant to the authorization of appropriations in para-
 13 graph (1) shall remain available until expended.

14 **TITLE II—ANTI-FRAUD**
 15 **PROTECTIONS**

16 **SEC. 201. PROTECTION FROM FRAUDULENT UNSOLICITED**
 17 **ELECTRONIC MAIL.**

18 (a) VIOLATIONS.—Subsection (a) of section 1030 of
 19 title 18, United States Code, as amended by section 101
 20 of this Act, is further amended by inserting after para-
 21 graph (7) the following new paragraph (8):

22 “(8) intentionally and without consent or au-
 23 thorization of the recipient initiates the transmission
 24 of an unsolicited commercial electronic mail adver-
 25 tisement to one or more protected computers with

1 knowledge that such advertisement falsifies an Inter-
 2 net domain, header information, date or time stamp,
 3 originating electronic mail address, or other identi-
 4 fier;”.

5 (b) PUNISHMENT.—Subsection (c)(2) of that section,
 6 as so amended, is further amended—

7 (1) in subparagraph (A)—

8 (A) by inserting “(i)” after “in the case of
 9 an offense”; and

10 (B) by inserting after “an offense punish-
 11 able under this subparagraph;” the following:
 12 “or (ii) under subsection (a)(8) which results in
 13 damage to a protected computer”; and

14 (2) by adding at the end the following new sub-
 15 paragraph:

16 “(D) in the case of a violation of subsection
 17 (a)(8), actual monetary loss and statutory damages
 18 of \$15,000 per violation, or an amount of up to \$10
 19 per message per violation whichever is greater;”.

20 (c) DEFINITIONS.—Subsection (c) of that section, as
 21 so amended, is further amended by adding after para-
 22 graph (12) the following new paragraphs:

23 “(13) the term ‘initiates the transmission’, in
 24 the case of an unsolicited commercial electronic mail
 25 advertisement, means to originate the commercial

1 electronic mail advertisement, and excludes the ac-
2 tions of any interactive computer service whose fa-
3 cilities or services are used by another person to
4 transmit, relay, or otherwise handle such advertise-
5 ment;

6 “(14) the term ‘Internet domain’ means a spe-
7 cific computer system (commonly referred to as a
8 ‘host’) or collection of computer systems attached to
9 or able to be referenced from the Internet which are
10 assigned a specific reference point on the Internet
11 (commonly referred to as an ‘Internet domain
12 name’) and registered with an organization recog-
13 nized by the Internet industry as a registrant of
14 Internet domains;

15 “(15) the term ‘unsolicited commercial elec-
16 tronic mail advertisement’ means any electronic mail
17 message or advertisement that is part of a plan, pro-
18 gram, or campaign conducted to induce purchases of
19 goods or services, but does not include electronic
20 mail initiated by any person to others with whom
21 such person has a prior relationship, including a
22 prior business relationship, or electronic mail sent by
23 a source to recipients where such recipients, or their
24 designees, have at any time affirmatively requested
25 to receive communications from that source; and

1 “(16) the term ‘Internet’ has the meaning given
2 that term in section 230(f)(1) of the Communica-
3 tions Act of 1934 (47 U.S.C. 230(f)(1)).”.

4 **TITLE III—PRIVACY AND CON-**
5 **FIDENTIALITY PROTECTIONS**

6 **SEC. 301. PRIVACY PROTECTION CONCERNING PEN REG-**
7 **ISTERS AND TRAP AND TRACE DEVICES.**

8 (a) ANNUAL REPORTS.—The text of section 3126 of
9 such title is amended to read as follows:

10 “(a) ANNUAL REPORTS.—The Attorney General shall
11 submit to Congress on an annual basis a report on the
12 exercise of the authority under this chapter with respect
13 to pen registers and trap and trace devices.

14 “(b) CONTENTS OF REPORTS.—Each report under
15 subsection (a) shall set forth, for the period covered by
16 such report, the following:

17 “(1) The number of orders for pen registers
18 and for trap and trace devices applied for by law en-
19 forcement agencies, and the number and duration of
20 any extensions of such orders.

21 “(2) The identity and location of the investiga-
22 tive or law enforcement agency making each applica-
23 tion.

24 “(3) The offense specified in each order or ap-
25 plication, or extension of order.

1 “(4) The number and nature of the facilities af-
2 fected.”.

3 (b) APPLICATIONS FOR ORDERS.—Section 3122(b) of
4 such title is amended—

5 (1) by striking “and” at the end of paragraph
6 (1);

7 (2) by striking the period at the end of para-
8 graph (2) and inserting “; and”; and

9 (3) by adding at the end the following new
10 paragraph:

11 “(3) a description of the facts on which the cer-
12 tification described in paragraph (2) is based.”.

13 **SEC. 302. PRIVACY PROTECTION FOR SUBSCRIBERS OF**
14 **SATELLITE TELEVISION SERVICES.**

15 (a) IN GENERAL.—Section 631 of the Communica-
16 tions Act of 1934 (47 U.S.C. 551) is amended by adding
17 at the end the following:

18 **“SEC. 631A. PRIVACY OF SUBSCRIBER INFORMATION FOR**
19 **SUBSCRIBERS OF SATELLITE TELEVISION**
20 **SERVICE.**

21 “(a) NOTICE TO SUBSCRIBERS REGARDING PERSON-
22 ALLY IDENTIFIABLE INFORMATION.—At the time of en-
23 tering into an agreement to provide any satellite home
24 viewing service to a subscriber, and not less often than
25 annually thereafter, a satellite carrier or distributor shall

1 provide notice in the form of a separate, written or elec-
2 tronic statement to the subscriber that clearly and con-
3 spicuously informs the subscriber of—

4 “(1) the nature of personally identifiable infor-
5 mation collected or to be collected with respect to
6 the subscriber as a result of the provision of such
7 service and the nature of the use of such informa-
8 tion;

9 “(2) the nature, frequency, and purpose of any
10 disclosure that may be made of such information, in-
11 cluding an identification of the types of persons to
12 whom the disclosure may be made;

13 “(3) the period during which such information
14 will be maintained by the satellite carrier or dis-
15 tributor;

16 “(4) the times and place at which the sub-
17 scriber may have access to such information in ac-
18 cordance with subsection (d); and

19 “(5) the limitations provided by this section
20 with respect to the collection and disclosure of infor-
21 mation by the satellite carrier or distributor and the
22 right of the subscriber under this section to enforce
23 such limitations.

24 “(b) COLLECTION OF PERSONALLY IDENTIFIABLE
25 INFORMATION.—

1 “(1) IN GENERAL.—Except as provided in para-
 2 graph (2), a satellite carrier or distributor shall not
 3 use its satellite system to collect personally identifi-
 4 able information concerning any subscriber without
 5 the prior written or electronic consent of such sub-
 6 scriber.

7 “(2) EXCEPTION.—A satellite carrier or dis-
 8 tributor may use its satellite system to collect infor-
 9 mation described in paragraph (1) in order—

10 “(A) to obtain information necessary to
 11 render a satellite service provided by the sat-
 12 ellite carrier or distributor to the subscriber; or

13 “(B) to detect unauthorized reception of
 14 satellite communications.

15 “(c) DISCLOSURE OF PERSONALLY IDENTIFIABLE
 16 INFORMATION.—

17 “(1) IN GENERAL.—Except as provided in para-
 18 graph (2), a satellite carrier or distributor—

19 “(A) may not disclose personally identifi-
 20 able information concerning any subscriber
 21 without the prior written or electronic consent
 22 of such subscriber; and

23 “(B) shall take such actions as are nec-
 24 essary to prevent unauthorized access to such

1 information by a person other than such sub-
2 scriber or the satellite carrier or distributor.

3 ~~“(2) EXCEPTIONS.—A satellite carrier or dis-~~
4 ~~tributor may disclose information described in para-~~
5 ~~graph (1) only if the disclosure is—~~

6 ~~“(A) necessary to render, or conduct a le-~~
7 ~~gitimate business activity related to, a cable or~~
8 ~~satellite service or other service provided by the~~
9 ~~satellite carrier or distributor to the subscriber;~~

10 ~~“(B) to a law enforcement agency pursu-~~
11 ~~ant to a warrant issued under the Federal~~
12 ~~Rules of Criminal Procedures, or equivalent~~
13 ~~State warrant, a Federal or State grand jury~~
14 ~~subpoena or equivalent process authorized by a~~
15 ~~Federal or State statute, or a court order~~
16 ~~issued in accordance with paragraph (3); and~~

17 ~~“(C) a disclosure of the names and ad-~~
18 ~~dresses of subscribers to any other provider of~~
19 ~~satellite service or other service, if—~~

20 ~~“(i) the satellite carrier or distributor~~
21 ~~has provided the subscriber the oppor-~~
22 ~~tunity to prohibit or limit such disclosure;~~
23 ~~and~~

24 ~~“(ii) the disclosure does not reveal, di-~~
25 ~~rectly or indirectly—~~

1 ~~“(I) the extent of any viewing or~~
2 ~~other use by the subscriber of satellite~~
3 ~~service or other service provided by~~
4 ~~the satellite carrier or distributor; or~~

5 ~~“(II) the nature of any trans-~~
6 ~~action made by the subscriber over~~
7 ~~the satellite system of the satellite~~
8 ~~carrier or distributor.~~

9 ~~“(3) COURT ORDERS.—~~

10 ~~“(A) LIMITATIONS.—(i) A disclosure under~~
11 ~~paragraph (2)(B) may be made only—~~

12 ~~“(I) with prior notice to the sub-~~
13 ~~scriber, except that delayed notice may be~~
14 ~~given pursuant to section 2705 of title 18,~~
15 ~~United States Code; and~~

16 ~~“(II) if the law enforcement agency~~
17 ~~shows that there is probable cause to be-~~
18 ~~lieve that the information sought is rel-~~
19 ~~evant to an ongoing criminal investigation~~
20 ~~being conducted by the agency.~~

21 ~~“(ii) In the case of a State government au-~~
22 ~~thority, such a court order shall not issue if~~
23 ~~prohibited by the law of such State.~~

24 ~~“(B) QUASH OR MODIFICATION.—A court~~
25 ~~issuing a court order pursuant to this para-~~

1 graph, on a motion made promptly by the sat-
2 ellite carrier or distributor, may quash or mod-
3 ify the order if the information requested is un-
4 reasonably voluminous in nature or if compli-
5 ance with the order otherwise would cause an
6 unreasonable burden on the satellite carrier or
7 distributor, as the case may be.

8 “(d) SUBSCRIBER ACCESS TO INFORMATION.—A sat-
9 ellite subscriber shall be provided access to all personally
10 identifiable information regarding that subscriber that is
11 collected and maintained by a satellite carrier or dis-
12 tributor. Such information shall be made available to the
13 subscriber at reasonable times and at a convenient place
14 designated by such satellite carrier or distributor. A sat-
15 ellite subscriber shall be provided reasonable opportunity
16 to correct any error in such information.

17 “(e) RELIEF.—

18 “(1) IN GENERAL.—Any person aggrieved by
19 any act of a satellite carrier or distributor in viola-
20 tion of this section may bring a civil action in a dis-
21 trict court of the United States.

22 “(2) DAMAGES AND COSTS.—In any action
23 brought under paragraph (1), the court may award
24 a prevailing plaintiff actual damages but not less
25 than liquidated damages computed at the rate of

1 \$100 a day for each day of violation or \$1,000,
2 whichever is greater.

3 “(f) DEFINITIONS.—In this section:

4 “(1) DISTRIBUTOR.—The term ‘distributor’ has
5 the meaning given that term in section 119(d)(1) of
6 title 17, United States Code.

7 “(2) OTHER SERVICE.—The term ‘other serv-
8 ice’ includes any wire, electronic, or radio commu-
9 nications service provided using any of the facilities
10 of a satellite carrier or distributor that are used in
11 the provision of satellite home viewing service.

12 “(3) PERSONALLY IDENTIFIABLE INFORMA-
13 TION.—The term ‘personally identifiable informa-
14 tion’ does not include any record of aggregate data
15 that does not identify particular persons.

16 “(4) SATELLITE CARRIER.—The term ‘satellite
17 carrier’ has the meaning given that term in section
18 119(d)(6) of title 17, United States Code.”.

19 (b) NOTICE WITH RESPECT TO CERTAIN AGREE-
20 MENTS.—

21 (1) IN GENERAL.—Except as provided in para-
22 graph (2), a satellite carrier or distributor who has
23 entered into agreements referred to in section
24 631(a) of the Communications Act of 1934, as
25 amended by subsection (a), before the date of enact-

1 ment of this Act, shall provide any notice required
2 under that section, as so amended, to subscribers
3 under such agreements not later than 180 days after
4 that date.

5 (2) **EXCEPTION.**—Paragraph (1) shall not
6 apply with respect to any agreement under which a
7 satellite carrier or distributor was providing notice
8 under section 631(a) of the Communications Act of
9 1934, as in effect on the day before the date of en-
10 actment of this Act, as of such date.

11 **SEC. 303. ENCRYPTION REPORTING REQUIREMENTS.**

12 Section 2519(2)(b) of title 18, United States Code,
13 is amended by striking “and (iv)” and inserting “(iv) the
14 number of orders in which encryption was encountered
15 and whether such encryption prevented law enforcement
16 from obtaining the plaintext of communications inter-
17 cepted pursuant to any such order; (v) the approximate
18 nature, amount, and cost of the manpower and other re-
19 sources used in obtaining the plaintext of intercepted com-
20 munications that were encrypted; and (vi)”.

21 **SEC. 304. FRAUD IN ONLINE COLLECTION AND DISSEMINA-**
22 **TION OF PERSONALLY IDENTIFIABLE INFOR-**
23 **MATION.**

24 Section 1030 of title 18, United States Code, as
25 amended by section 102(b) of this Act, is further amended

1 by inserting after subsection (i) the following new sub-
2 section (j):

3 “(j)(1) Except as otherwise provided in this sub-
4 section, an interactive computer service may not disclose
5 to a person other than the consumer concerned any per-
6 sonally identifiable information, unless—

7 “(A) the interactive computer service discloses
8 to the consumer, in a notice consistent with para-
9 graph (2), the types of persons to whom such infor-
10 mation may be disclosed; and

11 “(B) the consumer is given—

12 “(i) the opportunity, before the time that
13 such information is initially disclosed, to direct
14 that such information not be disclosed to such
15 person; and

16 “(ii) an explanation of how the consumer
17 can exercise that nondisclosure option available
18 under clause (i).

19 “(2) At the time of establishing a customer relation-
20 ship with a consumer and before collecting any personally
21 identifiable information from the consumer, an interactive
22 computer service shall provide to the consumer a disclo-
23 sure, which shall appear on the first webpage of the inter-
24 active computer service or be accessible by a hypertext link

1 from such first webpage, of the policies and practices of
2 the interactive computer service with respect to—

3 ~~“(A) the collection and use of personally identi-~~
4 ~~fiable information from customers who visit or use~~
5 ~~the website of the interactive computer service;~~

6 ~~“(B) the disclosure of such personally identifi-~~
7 ~~able information to persons other than such cus-~~
8 ~~tomers; and~~

9 ~~“(C) the protection of the confidentiality and~~
10 ~~security of such personally identifiable information.~~

11 ~~“(3) This subsection shall not prohibit the disclosure~~
12 ~~of personally identifiable information regarding a con-~~
13 ~~sumer if such disclosure is—~~

14 ~~“(A) with the consent or at the direction of the~~
15 ~~consumer (including the use of an electronic agent~~
16 ~~to provide such consent or direction);~~

17 ~~“(B) to protect the confidentiality or security of~~
18 ~~the records of the interactive computer service per-~~
19 ~~taining to the consumer;~~

20 ~~“(C) to protect against or prevent actual or po-~~
21 ~~tential fraud or unauthorized transactions;~~

22 ~~“(D) to persons holding a legal or beneficial in-~~
23 ~~terest relating to the consumer;~~

24 ~~“(E) to persons acting in a fiduciary or rep-~~
25 ~~resentative capacity on behalf of the consumer; or~~

1 “(F) required—

2 “(i) to comply with Federal, State, or local
3 laws or regulations, or other applicable legal re-
4 quirements;

5 “(ii) to comply with a properly authorized
6 civil, eriminal, or regulatory investigation or
7 subpoena by Federal, State, or local authorities;
8 or

9 “(iii) to respond to judicial process or gov-
10 ernment regulatory authorities for examination,
11 compliance, or other purposes as authorized by
12 law.

13 “(4) Nothing in this subsection may be construed to
14 prohibit an interactive computer service from using, dis-
15 closing, or permitting access to aggregate subscriber infor-
16 mation from which personally identifiable information has
17 been removed.

18 “(5) The Attorney General, any United States Attor-
19 ney, or any State Attorney General may maintain a civil
20 action against any person who violates this subsection for
21 appropriate civil or equitable relief.

22 “(6) In this subsection:

23 “(A) The term ‘consumer’ means an individual
24 who visits or transacts with an interactive computer
25 service for personal, family, or household purposes;

1 and also means the legal representative of such an
2 individual.

3 “(B) The term ‘customer’, with respect to an
4 interactive computer service, means any consumer
5 (or authorized representative of a consumer) of a
6 commercial product or service provided by such
7 interactive computer service.

8 “(C) the term ‘customer information of an
9 interactive computer service’ means any personally
10 identifiable information maintained by or for an
11 interactive computer service which is provided by a
12 customer to an interactive computer service.

13 “(D) The term ‘time of establishing a customer
14 relationship’ means the time when the website of an
15 interactive computer service is visited by a con-
16 sumer.

17 “(E) The term ‘interactive computer service’
18 means any person who—

19 “(i) operates, or on whose behalf is oper-
20 ated, a website located on the Internet or an
21 online service; and

22 “(ii) collects or maintains personal infor-
23 mation from or about the users of or visitors to
24 such website or online service, or on whose be-
25 half such information is collected or main-

1 tained; where such website or online service is
 2 operated for commercial purposes, including
 3 any person offering products or services for sale
 4 through that websites or online service, involv-
 5 ing commerce—

6 “(I) among the several States or with
 7 1 or more foreign nations; and

8 “(II) in any territory of the United
 9 States or in the District of Columbia, or
 10 between any such territory and—

11 “(aa) another such territory;

12 “(bb) any State or foreign na-
 13 tion; or

14 “(cc) between the District of Co-
 15 lumbia and any State, territory, or
 16 foreign nation.

17 “(F) The term ‘personally identifiable informa-
 18 tion’ means any of the following information pro-
 19 vided online by a consumer to an interactive com-
 20 puter service:

21 “(i) A first and last name.

22 “(ii) A home or other physical address, in-
 23 cluding a street name and name of a city or
 24 town.

25 “(iii) An electronic mail address.

1 “(iv) A telephone number.

2 “(v) A Social Security number.

3 “(vi) A credit card number or charge card,
4 and any related access code.

5 “(vii) A photograph.”.

6 **SEC. 305. NATIONAL MEDIA CAMPAIGN ON PUBLIC AWARE-**
7 **NESS REGARDING ONLINE SECURITY AND**
8 **PRIVACY.**

9 (a) NATIONAL MEDIA CAMPAIGN AUTHORIZED.—

10 (1) CAMPAIGN AUTHORIZED.—The Attorney
11 General, after consultation with the Deputy Assist-
12 ant Attorney General for Computer Crime and Intel-
13 lectual Property, may carry out a national media
14 campaign for purposes of raising public awareness of
15 existing rights, laws, and regulations relating to
16 Internet security and the privacy of personally iden-
17 tifiable information over the Internet.

18 (2) OUTSIDE ASSISTANCE.—The Attorney Gen-
19 eral may—

20 (A) carry out the campaign in cooperation
21 with appropriate non-Federal persons and enti-
22 ties; and

23 (B) seek and utilize non-Federal funds and
24 in-kind donations in carrying out the campaign.

1 (b) OBJECTIVES OF CAMPAIGN.—The objectives of
2 the campaign shall be—

3 (1) to heighten and increase public awareness
4 of the occurrence and extent of the collection and
5 dissemination of personally identifiable information,
6 and the security of such information, by commercial,
7 private, and public entities that maintain Internet
8 websites;

9 (2) to encourage Americans to learn of and be-
10 come familiar with actions that can be taken to pro-
11 tect their personally identifiable information from
12 being transferred without their consent or otherwise
13 misused by a third party;

14 (3) to inform Americans of their rights with re-
15 spect to their personally identifiable information;
16 and

17 (4) to inform Americans of Federal crimes re-
18 lating to computer fraud and abuse, and of the pun-
19 ishments for such crimes.

20 (c) ELEMENTS OF CAMPAIGN.—Subject to subsection
21 (d), the campaign shall be carried out through such means
22 as the Attorney General considers appropriate,
23 including—

24 (1) public service announcements;

25 (2) advertisements on television and radio;

1 ~~(3)~~ banners on the World Wide Web that are
 2 adoptable by commercial and community Internet
 3 websites;

4 ~~(4)~~ newspapers and magazines, including adver-
 5 tisements and submittals to editorial pages;

6 ~~(5)~~ out-of-home message sites, including bill-
 7 boards, posters, and signs;

8 ~~(6)~~ information through a toll-free telephone
 9 number (commonly referred to as an “800” num-
 10 ber); and

11 ~~(7)~~ other appropriate media and outlets.

12 ~~(d) LIMITATION ON USE OF FUNDS FOR CAM-~~
 13 ~~PAIGN.—~~

14 ~~(1) IN GENERAL.—~~No funds available for the
 15 campaign may be used as follows:

16 ~~(A)~~ To propose, influence, favor, or oppose
 17 any change in any statute, rule, regulation,
 18 treaty, or other provision of law.

19 ~~(B)~~ For any partisan political purpose.

20 ~~(C)~~ Except as provided in paragraph ~~(2)~~,
 21 to feature any elected official, person seeking
 22 elected office, cabinet-level official, or Federal
 23 official employed pursuant to Schedule C under
 24 section 213 of title 5, Code of Federal Regula-
 25 tions.

1 (D) In violation of section 1913 of title 18,
2 United States Code.

3 (2) EXCEPTION.—Funds available for the cam-
4 paign may be used as described in paragraph (1)(C)
5 if, not later than 15 days before the use of such
6 funds in that manner, a notice regarding the use of
7 such funds in that manner is submitted to the Com-
8 mittees on Appropriations and the Judiciary of the
9 Senate and House of Representatives.

10 (e) ASSESSMENT OF CAMPAIGN.—

11 (1) REQUIREMENT.—The Attorney General
12 shall enter into an agreement with a qualified cer-
13 tified public accountant for purposes of obtaining an
14 assessment of the campaign, including—

15 (A) an accounting of the amounts (includ-
16 ing Federal funds, other funds, and any in-kind
17 donations) received for purposes of conducting
18 the campaign; and

19 (B) an objective assessment of the effects
20 of the campaign, including the cost-effectiveness
21 of the campaign.

22 (2) REPORT.—The Attorney General shall sub-
23 mit to the Committees on Appropriations and the
24 Judiciary of the Senate and House of Representa-
25 tives a report on the assessment obtained under

1 paragraph (1). The report shall be submitted not
2 later than 270 days after the termination of the
3 campaign under subsection (f).

4 (g) AVAILABILITY OF FUNDS.—Of the amount
5 available for the campaign under subsection (h), not
6 more than an amount equal to 5 percent of such
7 amount shall be available to cover the costs of the
8 assessment obtained under this subsection.

9 (f) TERMINATION OF CAMPAIGN.—Activities under
10 the campaign, other than the assessment under subsection
11 (e), shall terminate not later than three years after the
12 date of the enactment of this Act.

13 (g) PERSONALLY IDENTIFIABLE INFORMATION DE-
14 FINED.—In this section, the term “personally identifiable
15 information”, has the meaning given that term in section
16 1030(j)(6)(F) of title 18, United States Code (as amended
17 by section 304(a) of this Act).

18 (h) AUTHORIZATION OF APPROPRIATION.—

19 (1) AUTHORIZATION.—There is hereby author-
20 ized to be appropriated for the Department of Jus-
21 tice for each of fiscal years 2001, 2002, and 2003,
22 \$25,000,000 for purposes of the campaign under
23 this section.

1 (2) AVAILABILITY.—Amounts appropriated pur-
2 suant to the authorization of appropriations in para-
3 graph (1) shall remain available until expended.

4 **SEC. 306. FRAUDULENT ACCESS TO PERSONALLY IDENTIFI-**
5 **ABLE INFORMATION.**

6 (a) IN GENERAL.—Section 1030 of title 18, United
7 States Code, as amended by this Act, is further amended
8 by inserting after subsection (j) the following new sub-
9 section (k):

10 “(k)(1) Except as provided in paragraphs (2) and
11 (3), whoever knowingly with intent to defraud obtains, or
12 causes to be disclosed to any person, personally identifi-
13 able information of an interactive computer service relat-
14 ing to another person without such person’s consent or
15 authorization—

16 “(A) by making a false, fictitious, or fraudulent
17 statement or representation to an officer, employee,
18 or agent of an interactive computer service;

19 “(B) by making a false, fictitious, or fraudulent
20 statement or representation to a customer of an
21 interactive computer service; or

22 “(C) by providing any document to an officer,
23 employee, or agent of an interactive computer serv-
24 ice, knowing that the document is forged, counter-
25 feit, or stolen, was fraudulently obtained, or contains

1 a false, fictitious, or fraudulent statement or rep-
2 resentation;

3 shall be punished as provided in subsection (e).

4 “(2) No provision of this subsection shall be con-
5 strued to prevent any interactive computer service, or any
6 officer, employee, or agent of an interactive computer serv-
7 ice, from obtaining personally identifiable information of
8 such interactive computer service in the course of—

9 “(A) testing the security procedures or systems
10 of such interactive computer service for maintaining
11 the confidentiality of personally identifiable informa-
12 tion;

13 “(B) investigating allegations of misconduct or
14 negligence on the part of any officer, employee, or
15 agent of such interactive computer service; or

16 “(C) recovering customer information of such
17 interactive computer service which was obtained or
18 received by another person in any manner described
19 in paragraph (1).

20 “(3) No provision of this section shall be construed
21 to prevent any insurance institution, or any officer, em-
22 ployee, or agency of an insurance institution, from obtain-
23 ing information as part of an insurance investigation into
24 criminal activity, fraud, material misrepresentation, or
25 material nondisclosure that is authorized for such institu-

1 tion under State law, regulation, interpretation, or
2 order.”.

3 (b) **ATTEMPTED OFFENSES.**—Subsection (b) of that
4 section is amended by striking “subsection (a)” and in-
5 serting “subsection (a) or (k)”.

6 **TITLE IV—NATIONAL SECURITY**
7 **AND CRITICAL INFRASTRUC-**
8 **TURE PROTECTION**

9 **SEC. 401. DEPUTY ASSISTANT ATTORNEY GENERAL FOR**
10 **COMPUTER CRIME AND INTELLECTUAL**
11 **PROPERTY.**

12 (a) **ESTABLISHMENT OF POSITION.**—(1) Chapter 31
13 of title 28, United States Code, is amended by inserting
14 after section 507 the following new section:

15 **“§ 507a. Deputy Assistant Attorney General for Com-**
16 **puter Crime and Intellectual Property**

17 “(a) The Attorney General shall appoint a Deputy
18 Assistant Attorney General for Computer Crime and Intel-
19 lectual Property.

20 “(b) The Deputy Assistant Attorney General shall be
21 the head of the Computer Crime and Intellectual Property
22 Section (CCIPS) of the Department of Justice.

23 “(c) The duties of the Deputy Assistant Attorney
24 General shall include the following:

1 “(1) To advise Federal prosecutors and law en-
2 forcement personnel regarding computer crime and
3 intellectual property crime.

4 “(2) To coordinate national and international
5 activities relating to combatting computer crime.

6 “(3) To provide guidance and assistance to
7 Federal, State, and local law enforcement agencies
8 and personnel, and appropriate foreign entities, re-
9 garding responses to threats of computer crime and
10 cyber-terrorism.

11 “(4) To serve as the liaison of the Attorney
12 General to the National Infrastructure Protection
13 Center (NIPC), the Department of Defense, the Na-
14 tional Security Agency, and the Central Intelligence
15 Agency on matters relating to computer crime.

16 “(5) To coordinate training for Federal, State,
17 and local prosecutors and law enforcement personnel
18 on laws pertaining to computer crime.

19 “(6) To propose and comment upon legislation
20 concerning computer crime, intellectual property
21 crime, encryption, electronic privacy, and electronic
22 commerce, and concerning the search and seizure of
23 computers.

24 “(7) Any other duties carried out by the head
25 of the Computer Crime and Intellectual Property

1 Section of the Department of Justice as of the date
2 of the enactment of the Internet Integrity and Crit-
3 ical Infrastructure Protection Act of 2000.

4 “(8) Such other duties as the Attorney General
5 considers appropriate.”.

6 (2) The table of sections at the beginning of such
7 chapter is amended by inserting after the item relating
8 to section 507 the following new item:

“507a. Deputy Assistant Attorney General for Computer Crime and Intellectual
Property.”.

9 (b) FIRST APPOINTMENT TO POSITION OF DEPUTY
10 ASSISTANT ATTORNEY GENERAL.—(1) The individual
11 who holds the position of head of the Computer Crime and
12 Intellectual Property Section (CCIPS) of the Department
13 of Justice as of the date of the enactment of this Act shall
14 act as the Deputy Assistant Attorney General for Com-
15 puter Crime and Intellectual Property under section 507a
16 of title 28, United States Code, until the Attorney General
17 appoints an individual to hold the position of Deputy As-
18 sistant Attorney General for Computer Crime and Intellec-
19 tual Property under that section.

20 (2) The individual first appointed as Deputy Assist-
21 ant Attorney General for Computer Crime and Intellectual
22 Property after the date of the enactment of this Act may
23 be the individual who holds the position of head of the

1 Computer Crime and Intellectual Property Section of the
2 Department of Justice as of that date.

3 (c) AUTHORIZATION OF APPROPRIATIONS FOR
4 CCIPS.—There is hereby authorized to be appropriated
5 for the Department of Justice for fiscal year 2001,
6 \$5,000,000 for the Computer Crime and Intellectual
7 Property Section of the Department for purposes of the
8 discharge of the duties of the Deputy Assistant Attorney
9 General for Computer Crime and Intellectual Property
10 under section 507a of title 28, United States Code (as so
11 added), during that fiscal year.

12 **SEC. 402. NATIONAL INFRASTRUCTURE PROTECTION CEN-**
13 **TER.**

14 (a) IN GENERAL.—The Director of the National In-
15 frastructure Protection Center (NPIC) within the Federal
16 Bureau of Investigation shall use amounts authorized to
17 be appropriated under subsection (b) for the following pur-
18 poses:

19 (1) To gather and analyze information con-
20 cerning threats to, and the vulnerability of, the na-
21 tional critical infrastructure.

22 (2) To provide assessments, warnings, and
23 emergency response information to other govern-
24 mental entities, and other owners and operators of

1 critical infrastructure, concerning threats to the na-
 2 tional critical infrastructure.

3 ~~(3) To provide assistance to law enforcement in~~
 4 ~~investigating and prosecuting attacks against the na-~~
 5 ~~tional critical infrastructure.~~

6 ~~(4) To develop and disseminate, in collaboration~~
 7 ~~with the private sector, technology and security pro-~~
 8 ~~cedures for shielding the national critical infrastruc-~~
 9 ~~ture against attack.~~

10 ~~(5) Such other purposes as the Director con-~~
 11 ~~siders appropriate.~~

12 ~~(b) AUTHORIZATION OF APPROPRIATIONS.—There is~~
 13 ~~hereby authorized to be appropriated for the Federal Bu-~~
 14 ~~reau of Investigation for the purposes set forth in sub-~~
 15 ~~section (a) the following:~~

16 ~~(1) For fiscal year 2001, \$45,000,000.~~

17 ~~(2) For each of fiscal years 2002 through 2005,~~
 18 ~~such sums as may be necessary for such fiscal years.~~

19 **SEC. 403. PERSONNEL EXCHANGE PROGRAMS FOR CRIT-**
 20 **ICAL INFRASTRUCTURE PROTECTION TRAIN-**
 21 **ING.**

22 Section 3371(4) of title 5, United States Code, is
 23 amended—

24 (1) by striking “or” at the end of subparagraph
 25 (C);

1 (2) by striking the period at the end of sub-
2 paragraph (D) and inserting “; or”; and

3 (3) by adding at the end the following new sub-
4 paragraph:

5 “(E) a provider of wire or electronic com-
6 munication service; provider of data encryption
7 or related services; or other entity; for the pur-
8 pose of furthering the objectives of the Internet
9 Integrity and Critical Infrastructure Protection
10 Act of 2000.”.

11 **TITLE V—INTERNATIONAL COM-**
12 **PUTER CRIME ENFORCE-**
13 **MENT**

14 **SEC. 501. SHORT TITLE.**

15 This title may be cited as the “International Com-
16 puter Crime Enforcement Assistance Act of 2000”.

17 **SEC. 502. DISCLOSURE OF COMPUTER CRIME EVIDENCE TO**
18 **FOREIGN LAW ENFORCEMENT AUTHORITIES**
19 **RELATING TO ENFORCEMENT OF FOREIGN**
20 **COMPUTER CRIME LAWS.**

21 (a) **IN GENERAL.**—Subject to subsection (b) and sec-
22 tion 505, the Attorney General of the United States may
23 provide computer crime (other than trade secrets or pro-
24 priety information otherwise not disclosable by the Attor-

1 ney General) to a foreign law enforcement authority to
 2 assist the foreign law enforcement authority—

3 (1) in determining whether a person has vio-
 4 lated or is about to violate a foreign computer crime
 5 law administered or enforced by the foreign law en-
 6 forcement authority; or

7 (2) in enforcing such a foreign computer crime
 8 law.

9 (b) **COMPUTER CRIME MUTUAL ASSISTANCE AGREE-**
 10 **MENT REQUIRED.**—The Attorney General may not pro-
 11 vide evidence to a foreign law enforcement authority under
 12 subsection (a) except pursuant to the provisions of a com-
 13 puter crime mutual assistance agreement with respect to
 14 the foreign law enforcement authority that is in effect
 15 under this title.

16 **SEC. 503. INVESTIGATIVE ASSISTANCE TO FOREIGN LAW**
 17 **ENFORCEMENT AUTHORITIES TO OBTAIN**
 18 **COMPUTER CRIME EVIDENCE RELATING TO**
 19 **ENFORCEMENT OF FOREIGN COMPUTER**
 20 **CRIME LAWS.**

21 (a) **IN GENERAL.**—Subject to the provisions of this
 22 section and section 505, the Attorney General of the
 23 United States may exercise any authority set forth in sub-
 24 section (b) to assist a foreign law enforcement authority—

1 (1) in determining whether a person has vio-
2 lated or is about to violate a foreign computer crime
3 law administered or enforced by the foreign law en-
4 forcement authority; or

5 (2) in enforcing such a foreign computer crime
6 law.

7 (b) COVERED AUTHORITIES.—

8 (1) IN GENERAL.—The authorities referred to
9 in this subsection are the authorities of the Attorney
10 General as follows:

11 (A) To investigate possible violations of the
12 Federal computer crime laws.

13 (B) To provide evidence obtained as a re-
14 sult of an investigation under subparagraph (A)
15 to the foreign law enforcement authority con-
16 cerned.

17 (2) SCOPE OF AUTHORITY.—An investigation
18 may be conducted under subparagraph (A) of para-
19 graph (1); and evidence obtained through such in-
20 vestigation may be provided under subparagraph (B)
21 of that paragraph, without regard to whether the
22 conduct investigated violates any Federal computer
23 crime law.

24 (c) COMPUTER CRIME MUTUAL ASSISTANCE AGREE-
25 MENT REQUIRED.—The Attorney General may not exer-

1 eise any authority set forth in subsection (b) on behalf
2 of a foreign law enforcement authority except pursuant to
3 the provisions of a computer crime mutual assistance
4 agreement with respect to the foreign law enforcement au-
5 thority that is in effect under this title.

6 (d) REQUESTS.—

7 (1) SUBMITTAL.—A foreign law enforcement
8 authority seeking the assistance of the Attorney
9 General under this section shall submit a request for
10 such assistance to the Attorney General.

11 (2) RESPONSE.—The Attorney General may ap-
12 prove or deny, in whole or in part, a request sub-
13 mitted under paragraph (1).

14 (3) PROHIBITION ON ACTION FOLLOWING DE-
15 NIAL.—The Attorney General may not take any ac-
16 tion under subsection (a) with respect to any part of
17 a request under this subsection that has been denied
18 by the Attorney General under paragraph (2).

19 (e) RIGHTS AND PRIVILEGES PRESERVED.—A per-
20 son may not be compelled in connection with an investiga-
21 tion under this section to give testimony or a statement,
22 or to produce a document or other thing, in violation of
23 any legally applicable right or privilege.

1 **SEC. 504. COURT ORDERS TO PROVIDE ASSISTANCE TO**
2 **FOREIGN LAW ENFORCEMENT AUTHORITIES**
3 **RELATING TO ENFORCEMENT OF FOREIGN**
4 **COMPUTER CRIME LAWS.**

5 (a) **AUTHORITY OF THE DISTRICT COURTS.**—On ap-
6 plication of the Attorney General of the United States
7 made in accordance with a computer crime mutual assist-
8 ance agreement in effect under this title, the United
9 States district court for the district in which a person re-
10 sides, is found, or transacts business may order the person
11 to give testimony or a statement, or to produce a docu-
12 ment or other thing, to the Attorney General in order to
13 assist a foreign law enforcement authority covered by the
14 agreement—

15 (1) in determining whether a person has vio-
16 lated or is about to violate a foreign computer crime
17 law administered or enforced by the foreign law en-
18 forcement authority; or

19 (2) in enforcing such a foreign computer crime
20 law.

21 (b) **LIMITATION ON APPLICATIONS.**—The making of
22 applications by the Attorney General under subsection (a)
23 is subject to the provisions of section 505.

24 (c) **CONTENTS OF ORDER.**—

25 (1) **USE OF APPOINTEE TO RECEIVE EVI-**
26 **DENCE.**—

1 (A) IN GENERAL.—An order issued under
2 subsection (a) may direct that testimony or a
3 statement be given, or a document or other
4 thing be produced, to a person who shall be rec-
5 ommended by the Attorney General and ap-
6 pointed by the court.

7 (B) POWERS.—A person appointed with
8 respect to an order under subparagraph (A)
9 shall have the power to administer any oath
10 necessary under the order and the power to
11 take testimony or statements.

12 (2) PRACTICE AND PROCEDURE.—

13 (A) IN GENERAL.—An order issued under
14 subsection (a) may prescribe the practice and
15 procedure for taking testimony and statements
16 and for producing documents and other things.

17 (B) SCOPE.—The practice and procedure
18 prescribed for an order under subparagraph (A)
19 may be in whole or in part the practice and
20 procedure of the foreign state, or the regional
21 economic integration organization, represented
22 by the foreign law enforcement authority with
23 respect to which the Attorney General requests
24 the order.

1 the Attorney General determines in the particular instance
2 that—

3 (1) the foreign law enforcement authority
4 concerned—

5 (A) will satisfy the assurances, terms, and
6 conditions under the agreement that are speci-
7 fied in paragraphs (1), (2), and (5) of section
8 508(b); and

9 (B) is capable of complying with and will
10 comply with the confidentiality requirements
11 applicable under the agreement with respect to
12 any requested computer crime evidence;

13 (2) providing any requested computer crime evi-
14 dence will not violate a limitation in section 508(e);
15 and

16 (3) disclosing the evidence, exercising the au-
17 thority, or applying for the order, as the case may
18 be, is consistent with the public interest of the
19 United States, taking into consideration whether the
20 foreign state or regional economic integration orga-
21 nization represented concerned holds any proprietary
22 interest that could benefit or otherwise be affected
23 by the disclosure, the exercise of the authority, or
24 the granting of the order.

1 (b) **LIMITATION ON DISCLOSURE OF CERTAIN COM-**
2 **PUTER CRIME EVIDENCE.**—The Attorney General may
3 not disclose in violation of a computer crime mutual assist-
4 ance agreement any computer crime evidence received
5 under the agreement, except that the agreement may not
6 prevent the disclosure of computer crime evidence to a de-
7 fendant in an action or proceeding brought by the Attor-
8 ney General for a violation of any Federal law if the disclo-
9 sure would otherwise be required by Federal law.

10 (c) **REQUIRED DISCLOSURE OF NOTICE RE-**
11 **CEIVED.**—If the Attorney General receives a notice de-
12 scribed in section 508(b)(8), the Attorney General shall
13 transmit the notice to the person that provided the evi-
14 dence with respect to which the notice is received.

15 **SEC. 506. REIMBURSEMENT.**

16 The Attorney General of the United States is author-
17 ized to receive from a foreign law enforcement authority,
18 or from the foreign state or regional economic integration
19 organization represented by such foreign law enforcement
20 authority, reimbursement of the costs incurred by the At-
21 torney General in disclosing evidence under section 502,
22 exercising any authority under section 503, or applying
23 for an order under section 504 with respect to a computer
24 crime mutual assistance agreement.

1 **SEC. 507. JUDICIAL REVIEW.**

2 (a) DETERMINATIONS.—A determination made under
3 paragraph (1), (2), or (3) of section 505(a) shall not be
4 subject to judicial review.

5 (b) CITATIONS TO AND DESCRIPTIONS OF CON-
6 FIDENTIALITY LAWS.—Whether a computer crime mutual
7 assistance agreement satisfies the requirement set forth
8 in section 508(b)(3) shall not be subject to judicial review.

9 (c) RULES OF CONSTRUCTION.—

10 (1) ADMINISTRATIVE PROCEDURE ACT.—The
11 requirements in section 508(d), with respect to pub-
12 lication and request for public comment, shall not be
13 construed to create any availability of judicial review
14 under chapter 7 of title 5, United States Code.

15 (2) EXCLUDED ELEMENTS.—Nothing in this
16 section shall be construed to affect the availability of
17 judicial review under laws referred to in section
18 508(e).

19 **SEC. 508. COMPUTER CRIME MUTUAL ASSISTANCE AGREE-**
20 **MENTS.**

21 (a) IN GENERAL.—

22 (1) DESCRIPTION GENERALLY.—Subject to the
23 provisions of this section, a computer crime mutual
24 assistance agreement for purposes of this title shall
25 consist of a written agreement, or written memo-
26 randum of understanding, that is entered into by the

1 United States and a foreign state or regional eco-
2 nomic integration organization with respect to the
3 foreign law enforcement authorities of the foreign
4 state or organization (and such other governmental
5 entities of the foreign state or organization as the
6 Attorney General determines may be necessary in
7 order to provide the assistance described in sub-
8 section (b)(1)) for purposes of carrying out activities
9 authorized by sections 502, 503, and 504, on a re-
10 ciprocal basis.

11 (2) OFFICIALS.—A computer crime mutual as-
12 sistance agreement shall be entered into jointly by
13 the Attorney General of the United States and a for-
14 eign law enforcement authority.

15 (b) ELEMENTS.—A computer crime mutual assist-
16 ance agreement shall contain the following elements:

17 (1) An assurance that any foreign law enforce-
18 ment authority covered by the agreement will pro-
19 vide to the Attorney General assistance that is com-
20 parable in scope to the assistance the Attorney Gen-
21 eral provides under the agreement.

22 (2) An assurance that any foreign law enforce-
23 ment authority covered by the agreement—

24 (A) is subject to laws and procedures that
25 are adequate to maintain securely the confiden-

1 tiality of computer crime evidence that may be
2 received under section 502, 503, or 504; and

3 (B) will give protection to such evidence
4 that is not less than the protection that would
5 be provided such evidence under the laws of the
6 United States.

7 (3) Citations to and brief descriptions of the
8 laws of the United States, and the laws of the for-
9 eign state or regional economic integration organiza-
10 tion concerned; that protect the confidentiality of
11 computer crime evidence that may be provided under
12 the agreement; which citations and descriptions shall
13 set forth the enforcement mechanisms and penalties
14 applicable under such laws and; in the case of a re-
15 gional economic integration organization, the appli-
16 cability of such laws; enforcement mechanisms; and
17 penalties to the foreign states composing the organi-
18 zation.

19 (4) Citations to the Federal computer crime
20 laws and the foreign computer crime laws with re-
21 spect to which the agreement applies.

22 (5) Terms and conditions that specifically re-
23 quire using; disclosing; or permitting the use or dis-
24 closure of computer crime evidence received under
25 the agreement only—

1 (A) for the purpose of administering or en-
2 forcing the foreign computer crime laws con-
3 cerned; or

4 (B) with respect to a specified disclosure
5 or use requested by a foreign law enforcement
6 authority and essential to a significant law en-
7 forcement objective, in accordance with the
8 prior written consent given by the Attorney
9 General after—

10 (i) determining that such computer
11 crime evidence is not otherwise readily
12 available with respect to such objective;

13 (ii) making the determinations de-
14 scribed in paragraphs (2) and (3) of sec-
15 tion 505(a), with respect to such disclosure
16 or use; and

17 (iii) making the determinations appli-
18 cable to a foreign law enforcement author-
19 ity under section 505(a)(1) (other than the
20 determination regarding the assurance de-
21 scribed in paragraph (1) of this sub-
22 section); with respect to each additional
23 governmental entity, if any, to be provided
24 such computer crime evidence in the course
25 of such disclosure or use, after having re-

1 received adequate written assurances applica-
2 ble to each such governmental entity.

3 (6) ~~An assurance that computer crime evidence~~
4 ~~received under section 502, 503, or 504 from the At-~~
5 ~~torney General, and all copies of such evidence, in~~
6 ~~the possession or control of any foreign law enforce-~~
7 ~~ment authority covered by the agreement will be re-~~
8 ~~turned to the Attorney General at the conclusion of~~
9 ~~the foreign investigation or proceeding with respect~~
10 ~~to which such evidence was so received.~~

11 (7) ~~Terms and conditions that specifically pro-~~
12 ~~vide that the agreement will be terminated if—~~

13 (A) ~~the confidentiality required under the~~
14 ~~agreement is violated with respect to computer~~
15 ~~crime evidence; and~~

16 (B) ~~adequate action is not taken to mini-~~
17 ~~mize any harm resulting from such violation~~
18 ~~and to ensure that the confidentiality required~~
19 ~~under the agreement is not violated again.~~

20 (8) ~~Terms and conditions that specifically pro-~~
21 ~~vide that if the confidentiality required under the~~
22 ~~agreement is violated with respect to computer crime~~
23 ~~evidence, notice of the violation will be given—~~

24 (A) ~~by the foreign law enforcement author-~~
25 ~~ity concerned promptly to the Attorney General~~

1 with respect to computer crime evidence pro-
2 vided by the Attorney General; and

3 ~~(B)~~ by the Attorney General to the person
4 (if any) that provided such evidence to the At-
5 torney General.

6 ~~(c)~~ EXCLUSIONS.—A computer crime mutual assist-
7 ance agreement may not cover any of the following com-
8 puter crime evidence:

9 (1) Computer crime evidence in a matter occur-
10 ring before a grand jury and with respect to which
11 disclosure is prevented by Federal law, except that
12 for the purpose of applying Rule 6(e)(3)(C)(iv) of
13 the Federal Rules of Criminal Procedure with re-
14 spect to this paragraph—

15 ~~(A)~~ a foreign law enforcement authority
16 with respect to which a particularized need for
17 such computer crime evidence is shown shall be
18 considered to be an appropriate official of any
19 of the several States; and

20 ~~(B)~~ a foreign computer crime law adminis-
21 tered or enforced by the foreign law enforce-
22 ment authority shall be considered to be a State
23 criminal law.

24 ~~(2)~~ Computer crime evidence that is specifically
25 authorized under an Executive Order to be kept se-

1 eret in the interest of national defense or foreign
2 policy and—

3 (A) that is classified pursuant to such
4 order or a successor order; or

5 (B) with respect to which a determination
6 of classification is pending under such order or
7 successor order.

8 (3) Computer crime evidence that is classified
9 under the Atomic Energy Act of 1954 (42 U.S.C.
10 2011 et seq.).

11 (d) PUBLICATION REQUIREMENTS.—

12 (1) PRIOR TO ENTRY.—Not later than 45 days
13 before a computer crime mutual assistance agree-
14 ment is entered into for purposes of this title, the
15 Attorney General shall publish in the Federal
16 Register—

17 (A) the proposed text of the agreement;

18 and

19 (B) a request for public comment with re-
20 spect to the text.

21 (2) PRIOR TO MODIFICATION.—Not later than
22 45 days before the entry into any agreement that
23 makes a modification of a computer crime mutual
24 assistance agreement for purposes of this title, the

1 Attorney General shall publish in the Federal
2 Register—

3 (A) the proposed text of the modification;

4 and

5 (B) a request for public comment with re-
6 spect to the modification.

7 ~~(3) OTHER SIGNIFICANT EVENTS.—~~Not later
8 than 45 days after a computer crime mutual assist-
9 ance agreement for purposes of this title is entered
10 into or terminated, or an agreement that makes a
11 modification of a computer crime mutual assistance
12 agreement is entered into, the Attorney General
13 shall publish in the Federal Register—

14 (A) the text of the agreement or modifica-
15 tion, or the terms of the termination, as the
16 case may be; and

17 (B) in the case of an agreement that
18 makes a modification to a computer crime mu-
19 tual assistance agreement, a notice
20 containing—

21 (i) citations to the locations of publi-
22 cation in the Federal Register of the text
23 of the computer crime mutual assistance
24 agreement that is so modified, and of any

1 previous modification to such agreement;
2 and

3 (ii) a description of the manner in
4 which a copy of the computer crime mutual
5 assistance agreement, as so modified, may
6 be obtained from the Attorney General.

7 (4) **CONDITION FOR VALIDITY.**—A computer
8 crime mutual assistance agreement, or an agreement
9 that makes a modification to a computer crime mu-
10 tual assistance agreement, with respect to which
11 publication does not occur in accordance with para-
12 graph (1), (2), or (3), as applicable, shall not be
13 considered to be in effect for purposes of this title.

14 **SEC. 509. PRESERVATION OF EXISTING AUTHORITY.**

15 The authority provided by this title is in addition to
16 any other authority vested in the Attorney General of the
17 United States, or any other officer of the United States.

18 **SEC. 510. REPORT TO CONGRESS.**

19 Not later than 3 years after the date of the enact-
20 ment of this Act, the Attorney General of the United
21 States shall submit to the Committees on the Judiciary
22 of the Senate and House of Representatives a report—

23 (1) describing the effects of the operation of
24 this title on the enforcement of the Federal com-
25 puter crime laws;

1 (2) describing the extent to which foreign law
2 enforcement authorities have complied with the con-
3 fidentiality requirements applicable under computer
4 crime mutual assistance agreements in effect for
5 purposes of this title;

6 (3) specifying separately the identities of the
7 foreign states and regional economic integration or-
8 ganizations that have entered into such agreements
9 and the identities of the foreign law enforcement au-
10 thorities with respect to which such foreign states
11 and organizations have entered into such agree-
12 ments;

13 (4) specifying the identity of each foreign state,
14 and each regional economic integration organization,
15 that has in effect a law similar to this title;

16 (5) setting forth the approximate number of re-
17 quests made by the Attorney General under such
18 agreements to foreign law enforcement authorities
19 for computer crime investigations and for computer
20 crime evidence;

21 (6) setting forth the approximate number of re-
22 quests made to the Attorney General by foreign law
23 enforcement authorities under such agreements for
24 disclosures of evidence under section 502, the exer-

1 eise of any authority under section 503, or for appli-
2 cations for orders under section 504; and

3 (7) describing any significant problems or con-
4 cerns of which the Attorney General is aware with
5 respect to the operation of this title.

6 **SEC. 511. DEFINITIONS.**

7 In this title:

8 (1) **COMPUTER CRIME EVIDENCE.**—The term
9 “computer crime evidence” means information, testi-
10 mony, statements, documents, or other things that
11 are obtained in anticipation of, or during the course
12 of, an investigation or proceeding under any Federal
13 computer crime law or foreign computer crime law.

14 (2) **FEDERAL COMPUTER CRIME LAW.**—The
15 term “Federal computer crime law” means any law
16 designated by the Attorney General as a Federal
17 computer crime law under regulations prescribed by
18 the Attorney General for purposes of this title not
19 later than 90 days after the date of the enactment
20 of this Act and modified by the Attorney General
21 from time to time after notice to Congress of such
22 modification.

23 (3) **FOREIGN COMPUTER CRIME LAW.**—The
24 term “foreign computer crime law” means a law of
25 a foreign state, or of a regional economic integration

1 organization, that is substantially similar to a Fed-
2 eral computer crime law and prohibits conduct simi-
3 lar to conduct prohibited by a Federal computer
4 crime law.

5 (4) FOREIGN LAW ENFORCEMENT AUTHOR-
6 ITY.—The term “foreign law enforcement authority”
7 means a governmental entity of a foreign state or re-
8 gional economic integration organization that is vest-
9 ed by such state or organization with authority to
10 enforce the foreign computer crime laws of such
11 state or organization.

12 (5) REGIONAL ECONOMIC INTEGRATION ORGA-
13 NIZATION.—The term “regional economic integra-
14 tion organization” means an organization—

15 (A) that is constituted by, and composed
16 of, foreign states; and

17 (B) on which such foreign states have con-
18 ferred sovereign authority to make decisions
19 that are binding on such foreign states and di-
20 rectly applicable to and binding on persons
21 within such foreign states, including decisions
22 with respect to—

23 (i) administering or enforcing the for-
24 eign computer crime laws of such organiza-
25 tion; and

1 (ii) prohibiting and regulating disclo-
 2 sure of information that is obtained by
 3 such organization in the course of admin-
 4 istering or enforcing such laws.

5 **TITLE VI—SEVERABILITY**

6 **SEC. 601. SEVERABILITY.**

7 If any provision of this Act (including an amendment
 8 made by this Act), or the application thereof, to any per-
 9 son or circumstance, is held invalid, the remainder of this
 10 Act (including the amendments made by this Act), and
 11 the application thereof, to other persons or circumstances
 12 shall not be affected thereby.

13 **SECTION 1. SHORT TITLE.**

14 *This Act may be cited as the “Internet Integrity and*
 15 *Critical Infrastructure Protection Act of 2000”.*

16 **SEC. 2. DEPUTY ASSISTANT ATTORNEY GENERAL FOR COM-** 17 **PUTER CRIME AND INTELLECTUAL PROP-** 18 **ERTY.**

19 *(a) ESTABLISHMENT OF POSITION.—(1) Chapter 31 of*
 20 *title 28, United States Code, is amended by inserting after*
 21 *section 507 the following new section:*

1 **“§507a. Deputy Assistant Attorney General for Com-**
2 **puter Crime and Intellectual Property**

3 *“(a) The Attorney General shall appoint a Deputy As-*
4 *stant Attorney General for Computer Crime and Intellec-*
5 *tual Property.*

6 *“(b) The Deputy Assistant Attorney General shall be*
7 *the head of the Computer Crime and Intellectual Property*
8 *Section (CCIPS) of the Department of Justice.*

9 *“(c) The duties of the Deputy Assistant Attorney Gen-*
10 *eral shall include the following:*

11 *“(1) To advise Federal prosecutors and law en-*
12 *forcement personnel regarding computer crime and*
13 *intellectual property crime.*

14 *“(2) To coordinate national and international*
15 *law enforcement activities relating to combatting*
16 *computer crime.*

17 *“(3) To provide guidance and assistance to Fed-*
18 *eral, State, and local law enforcement agencies and*
19 *personnel, and appropriate foreign entities, regarding*
20 *responses to threats of computer crime and cyber-ter-*
21 *rorism.*

22 *“(4) To serve as the liaison of the Attorney Gen-*
23 *eral to the National Infrastructure Protection Center*
24 *(NIPC), the Department of Defense, the National Se-*
25 *curity Agency, and the Central Intelligence Agency on*
26 *matters relating to computer crime.*

1 “(5) *To coordinate training for Federal, State,*
 2 *and local prosecutors and law enforcement personnel*
 3 *on laws pertaining to computer crime.*

4 “(6) *To propose and comment upon legislation*
 5 *concerning computer crime, intellectual property*
 6 *crime, encryption, electronic privacy, and electronic*
 7 *commerce, and concerning the search and seizure of*
 8 *computers.*

9 “(7) *Such other duties as the Attorney General*
 10 *may require, including duties carried out by the head*
 11 *of the Computer Crime and Intellectual Property Sec-*
 12 *tion of the Department of Justice as of the date of the*
 13 *enactment of the Internet Integrity and Critical In-*
 14 *frastructure Protection Act of 2000.”.*

15 (2) *The table of sections at the beginning of such chap-*
 16 *ter is amended by inserting after the item relating to section*
 17 *507 the following new item:*

*“507a. Deputy Assistant Attorney General for Computer Crime and Intellectual
 Property.”.*

18 (b) *FIRST APPOINTMENT TO POSITION OF DEPUTY AS-*
 19 *SISTANT ATTORNEY GENERAL.—(1) The individual who*
 20 *holds the position of head of the Computer Crime and Intel-*
 21 *lectual Property Section (CCIPS) of the Department of Jus-*
 22 *tice as of the date of the enactment of this Act shall act*
 23 *as the Deputy Assistant Attorney General for Computer*
 24 *Crime and Intellectual Property under section 507a of title*

1 28, *United States Code*, until the Attorney General appoints
 2 an individual to hold the position of Deputy Assistant At-
 3 torney General for Computer Crime and Intellectual Prop-
 4 erty under that section.

5 (2) *The individual first appointed as Deputy Assistant*
 6 *Attorney General for Computer Crime and Intellectual*
 7 *Property after the date of the enactment of this Act may*
 8 *be the individual who holds the position of head of the Com-*
 9 *puter Crime and Intellectual Property Section of the De-*
 10 *partment of Justice as of that date.*

11 (c) *AUTHORIZATION OF APPROPRIATIONS FOR*
 12 *CCIPS.—There is hereby authorized to be appropriated for*
 13 *the Department of Justice for fiscal year 2001, \$5,000,000*
 14 *for the Computer Crime and Intellectual Property Section*
 15 *of the Department for purposes of the discharge of the duties*
 16 *of the Deputy Assistant Attorney General for Computer*
 17 *Crime and Intellectual Property under section 507a of title*
 18 *28, United States Code (as so added), during that fiscal*
 19 *year.*

20 **SEC. 3. DETERRENCE AND PREVENTION OF FRAUD, ABUSE,**
 21 **AND CRIMINAL ACTS IN CONNECTION WITH**
 22 **COMPUTERS.**

23 (a) *CLARIFICATION OF PROTECTION OF PROTECTED*
 24 *COMPUTERS.—Subsection (a)(5) of section 1030 of title 18,*
 25 *United States Code, is amended—*

1 (1) by inserting “(i)” after “(A)”;

2 (2) by redesignated subparagraphs (B) and (C)
3 as clauses (ii) and (iii), respectively, of subparagraph
4 (A);

5 (3) by adding “and” at the end of clause (iii),
6 as so redesignated; and

7 (4) by adding at the end the following new sub-
8 paragraph:

9 “(B) the conduct described in clause (i), (ii), or
10 (iii) of subparagraph (A) caused (or, in the case of
11 an attempted offense, would, if completed, have
12 caused)—

13 “(i) loss to 1 or more persons during any
14 1-year period (including loss resulting from a re-
15 lated course of conduct affecting 1 or more other
16 protected computers) aggregating at least \$5,000
17 in value;

18 “(ii) the modification or impairment, or
19 potential modification or impairment, of the
20 medical examination, diagnosis, treatment, or
21 care of 1 or more individuals;

22 “(iii) physical injury to any person;

23 “(iv) a threat to public health or safety; or

24 “(v) damage affecting a computer system
25 used by or for a government entity in further-

1 *ance of the administration of justice, national*
 2 *defense, or national security;”.*

3 **(b) PROTECTION FROM EXTORTION.**—Subsection
 4 *(a)(7) of that section is amended by striking “, firm, asso-*
 5 *ciation, educational institution, financial institution, gov-*
 6 *ernmental entity, or other legal entity,”.*

7 **(c) PENALTIES.**—Subsection (c) of that section is
 8 *amended—*

9 **(1) in paragraph (2)—**

10 **(A) in subparagraph (A)—**

11 *(i) by inserting “except as provided in*
 12 *subparagraph (B),” before “a fine”;*

13 *(ii) by striking “(a)(5)(C)” and insert-*
 14 *ing “(a)(5)(A)(iii); and*

15 *(iii) by striking “and” at the end;*

16 **(B) in subparagraph (B), by inserting “or**
 17 *an attempt to commit an offense punishable*
 18 *under this subparagraph,” after “subsection*
 19 *(a)(2),” in the matter preceding clause (i); and*

20 **(C) in subparagraph (C), by striking “and”**
 21 *at the end;*

22 **(2) in paragraph (3)—**

23 **(A) by striking “, (a)(5)(A), (a)(5)(B),”**
 24 *both places it appears; and*

25 **(B) by striking “and” at the end; and**

1 (3) by adding at the end the following new para-
2 graphs:

3 “(4)(A) a fine under this title, imprisonment for
4 not more than 10 years, or both, in the case of an of-
5 fense under subsection (a)(5)(A)(i), or an attempt to
6 commit an offense punishable under this subpara-
7 graph;

8 “(B) a fine under this title, imprisonment for
9 not more than 5 years, or both, in the case of an of-
10 fense under subsection (a)(5)(A)(ii), or an attempt to
11 commit an offense punishable under this subpara-
12 graph;

13 “(C) a fine under this title, imprisonment for
14 not more than 20 years, or both, in the case of an of-
15 fense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or
16 an attempt to commit an offense punishable under
17 this subparagraph, that occurs after a conviction for
18 another offense under this section; and

19 “(5) in the case of any felony offense under this
20 section, at the discretion of the court, termination of
21 and ineligibility for any financial assistance for edu-
22 cation at a post-secondary institution that is avail-
23 able under Federal law, which punishment shall be in
24 addition to any other punishment described in this
25 subsection.”.

1 (d) *DEFINITIONS.*—*Subsection (e) of that section is*
2 *amended—*

3 (1) *in paragraph (2)(B), by inserting “, includ-*
4 *ing a computer located outside the United States” be-*
5 *fore the semicolon;*

6 (2) *in paragraph (7), by striking “and” at the*
7 *end;*

8 (3) *by striking paragraph (8) and inserting the*
9 *following new paragraph (8):*

10 “(8) *the term ‘damage’ means any impairment*
11 *to the integrity or availability of data, a program, a*
12 *system, or information;”*

13 (4) *in paragraph (9), by striking the period at*
14 *the end and inserting a semicolon; and*

15 (5) *by adding at the end the following new para-*
16 *graphs:*

17 “(10) *the term ‘conviction’ shall include—*

18 “(A) *an adjudication of juvenile delin-*
19 *quency for a violation of this section; and*

20 “(B) *a conviction under the law of any*
21 *State for a crime punishable by imprisonment*
22 *for more than 1 year, an element of which is un-*
23 *authorized access, or exceeding authorized access,*
24 *to a computer;*

1 “(11) the term ‘loss’ means any reasonable cost
2 to any victim, including the cost of responding to an
3 offense, conducting a damage assessment, and restor-
4 ing the data, program, system, or information to its
5 condition prior to the offense, and any revenue lost,
6 cost incurred, or other consequential damages in-
7 curred because of interruption of service;

8 “(12) the term ‘person’ means any individual,
9 firm, corporation, educational institution, financial
10 institution, governmental entity, or legal or other en-
11 tity;”.

12 (e) *DAMAGES IN CIVIL ACTIONS*.—Subsection (g) of
13 that section is amended—

14 (1) by striking the second sentence and inserting
15 the following new sentences: “A suit for a violation of
16 subsection (a)(5) may be brought only if the conduct
17 involves one of the factors enumerated in subsection
18 (a)(5)(B). Damages for a violation involving only
19 conduct described in subsection (a)(5)(B)(i) are lim-
20 ited to economic damages.”; and

21 (2) by adding at the end the following new sen-
22 tence: “No action may be brought under this sub-
23 section for the negligent design or manufacture of
24 computer hardware, computer software, or
25 firmware.”.

1 **SEC. 4. CRIMINAL AND CIVIL FORFEITURE FOR COMPUTER**
2 **FRAUD AND ABUSE.**

3 (a) *CRIMINAL FORFEITURE.*—Section 1030 of title 18,
4 *United States Code, as amended by section 102 of this Act,*
5 *is further amended—*

6 (1) *by redesignating subsection (h) as subsection*
7 *(l); and*

8 (2) *by inserting after subsection (g) the following*
9 *new subsection (h):*

10 “(h)(1) *The court, in imposing sentence on any person*
11 *convicted of a violation of this section, shall order, in addi-*
12 *tion to any other sentence imposed and irrespective of any*
13 *provision of State law, that such person forfeit to the United*
14 *States—*

15 “(A) *the interest of such person in any personal*
16 *property that was used or intended to be used to com-*
17 *mit or to facilitate the commission of such violation;*
18 *and*

19 “(B) *any property, whether real or personal,*
20 *constituting or derived from any proceeds that such*
21 *person obtained, whether directly or indirectly, as a*
22 *result of such violation.*

23 “(2) *The criminal forfeiture of property under this*
24 *subsection, any seizure and disposition thereof, and any ad-*
25 *ministrative or judicial proceeding relating thereto, shall*
26 *be governed by the provisions of section 413 of the Com-*

1 *prehensive Drug Abuse Prevention and Control Act of 1970*
 2 *(21 U.S.C. 853), except subsection (d) of that section.”.*

3 *(b) CIVIL FORFEITURE.—That section, as amended by*
 4 *subsection (a) of this section, is further amended by insert-*
 5 *ing after subsection (h) the following new subsection (i):*

6 *“(i)(1) The following shall be subject to forfeiture to*
 7 *the United States, and no property right shall exist in them:*

8 *“(A) Any personal property that is used or in-*
 9 *tended to be used to commit or to facilitate the com-*
 10 *mission of any violation of this section.*

11 *“(B) Any property, whether real or personal,*
 12 *that constitutes or is derived from proceeds traceable*
 13 *to any violation of this section.*

14 *“(2) The provisions of chapter 46 of this title relating*
 15 *to civil forfeiture shall apply to any seizure or civil for-*
 16 *feiture under this subsection.”.*

17 **SEC. 5. ENHANCED COORDINATION OF FEDERAL AGENCIES.**

18 *Section 1030(d) of title 18, United States Code, is*
 19 *amended—*

20 *(1) by striking “subsections (a)(2)(A), (a)(2)(B),*
 21 *(a)(3), (a)(4), (a)(5), and (a)(6) of”; and*

22 *(2) by striking “which shall be entered into by”*
 23 *and inserting “between”.*

1 **SEC. 6. JUVENILE INVOLVEMENT IN COMPUTER CRIMES.**

2 *Section 5032 of title 18, United States Code, is amend-*
3 *ed in clause (3) of the first undesignated paragraph—*

4 *(1) by striking “or section 1002(a)” and insert-*
5 *ing “section 1002(a)”;* and

6 *(2) by inserting after “of this title,” the fol-*
7 *lowing: “or is a violation of section 1030(a)(1),*
8 *(a)(2)(B), (a)(3), or (a)(5)(A)(i) of this title,”.*

9 **SEC. 7. ADDITIONAL DEFENSE TO CIVIL ACTIONS RELATING**
10 **TO PRESERVING RECORDS IN RESPONSE TO**
11 **GOVERNMENT REQUESTS.**

12 *Section 2707(e)(1) of title 18, United States Code, is*
13 *amended by inserting after “or statutory authorization” the*
14 *following: “(including a request of a governmental entity*
15 *under section 2703(f) of this title)”.*

16 **SEC. 8. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELEC-**
17 **TRONIC COMMUNICATIONS RELATING TO**
18 **COMPUTER FRAUD AND ABUSE.**

19 *Section 2516(1)(c) of title 18, United States Code, is*
20 *amended by striking “and section 1341 (relating to mail*
21 *fraud),” and inserting “section 1341 (relating to mail*
22 *fraud), a felony violation of section 1030 (relating to com-*
23 *puter fraud and abuse),”.*

1 **SEC. 9. FORFEITURE OF DEVICES USED IN COMPUTER**
2 **SOFTWARE COUNTERFEITING AND INTELLEC-**
3 **TUAL PROPERTY THEFT.**

4 (a) *IN GENERAL.*—Section 2318(d) of title 18, United
5 States Code, is amended—

6 (1) by inserting “(1)” before “When”;

7 (2) in paragraph (1), as so designated, by insert-
8 ing “, and of any replicator or other device or thing
9 used to copy or produce the computer program or
10 other item to which the counterfeit labels have been af-
11 fixed or which were intended to have had such labels
12 affixed” before the period; and

13 (3) by adding at the end the following:

14 “(2) The forfeiture of property under this section, in-
15 cluding any seizure and disposition of the property, and
16 any related judicial or administrative proceeding, shall be
17 governed by the provisions of section 413 (other than sub-
18 section (d) of that section) of the Comprehensive Drug Abuse
19 Prevention and Control Act of 1970 (21 U.S.C. 853).”.

20 (b) *CONFORMING AMENDMENT.*—Section 492 of such
21 title is amended in the first undesignated paragraph by
22 striking “or 1720,” and inserting “, 1720, or 2318”.

23 **SEC. 10. SENTENCING DIRECTIVES FOR COMPUTER**
24 **CRIMES.**

25 (a) *AMENDMENT OF SENTENCING GUIDELINES RELAT-*
26 *ING TO CERTAIN COMPUTER CRIMES.*—Pursuant to its au-

1 *thority under section 994(p) of title 28, United States Code,*
2 *the United States Sentencing Commission shall amend the*
3 *Federal sentencing guidelines and, if appropriate, shall*
4 *promulgate guidelines or policy statements or amend exist-*
5 *ing policy statements to address—*

6 (1) *the potential and actual loss resulting from*
7 *an offense under section 1030 of title 18, United*
8 *States Code (as amended by this Act);*

9 (2) *the level of sophistication and planning in-*
10 *volved in such an offense;*

11 (3) *the growing incidence of offenses under such*
12 *subsections and the need to provide an effective deter-*
13 *rent against such offenses;*

14 (4) *whether or not such an offense was com-*
15 *mitted for purposes of commercial advantage or pri-*
16 *vate financial benefit;*

17 (5) *whether or not the defendant involved a juve-*
18 *nile in the commission of such an offense;*

19 (6) *whether or not the defendant acted with ma-*
20 *licious intent to cause harm in committing such an*
21 *offense;*

22 (7) *the extent to which such an offense violated*
23 *the privacy rights of individuals harmed by the of-*
24 *fense; and*

1 (8) *any other factor the Commission considers*
2 *appropriate in connection with any amendments*
3 *made by this Act with regard to such subsections.*

4 **(b) AMENDMENT OF SENTENCING GUIDELINES RELAT-**
5 **ING TO CERTAIN COMPUTER FRAUD AND ABUSE.—***Pursu-*
6 *ant to its authority under section 994(p) of title 28, United*
7 *States Code, the United States Sentencing Commission*
8 *shall amend the Federal sentencing guidelines to ensure that*
9 *any individual convicted of a violation of section*
10 *1030(a)(5)(A)(ii) or 1030(a)(5)(A)(iii) of title 18, United*
11 *States Code (as amended by section 3 of this Act), can be*
12 *subjected to appropriate penalties, without regard to any*
13 *mandatory minimum term of imprisonment.*

14 **(c) AMENDMENT OF SENTENCING GUIDELINES RELAT-**
15 **ING TO USE OF ENCRYPTION.—***Pursuant to its authority*
16 *under section 994(p) of title 28, United States Code, the*
17 *United States Sentencing Commission shall amend the Fed-*
18 *eral sentencing guidelines and, if appropriate, shall pro-*
19 *mulgate guidelines or policy statements or amend existing*
20 *policy statements to ensure that the guidelines provide suffi-*
21 *ciently stringent penalties to deter and punish persons who*
22 *intentionally use encryption in connection with the com-*
23 *mission or concealment of criminal acts sentenced under the*
24 *guidelines.*

1 (d) *EMERGENCY AUTHORITY.*—*The Commission may*
 2 *promulgate the guidelines or amendments provided for*
 3 *under this section in accordance with the procedures set*
 4 *forth in section 21(a) of the Sentencing Act of 1987, as*
 5 *though the authority under that Act had not expired.*

6 **SEC. 11. ASSISTANCE TO FEDERAL, STATE, AND LOCAL**
 7 **COMPUTER CRIME ENFORCEMENT AND ES-**
 8 **TABLISHMENT OF NATIONAL CYBER CRIME**
 9 **TECHNICAL SUPPORT CENTER.**

10 (a) *NATIONAL CYBER CRIME TECHNICAL SUPPORT*
 11 *CENTER.*—

12 (1) *CONSTRUCTION REQUIRED.*—*The Director of*
 13 *the Federal Bureau of Investigation shall provide for*
 14 *the construction and equipping of the technical sup-*
 15 *port center of the Federal Bureau of Investigation re-*
 16 *ferred to in section 811(a)(1)(A) of the Antiterrorism*
 17 *and Effective Death Penalty Act of 1996 (Public Law*
 18 *104–132; 110 Stat. 1312; 28 U.S.C. 531 note).*

19 (2) *NAMING.*—*The technical support center con-*
 20 *structed and equipped under paragraph (1) shall be*
 21 *known as the “National Cyber Crime Technical Sup-*
 22 *port Center”.*

23 (3) *FUNCTIONS.*—*In addition to any other au-*
 24 *thorized functions, the functions of the National Cyber*
 25 *Crime Technical Support Center shall be—*

1 (A) to serve as a centralized technical re-
2 source for Federal, State, and local law enforce-
3 ment and to provide technical assistance in the
4 investigation of computer-related criminal ac-
5 tivities;

6 (B) to assist Federal, State, and local law
7 enforcement in enforcing Federal, State, and
8 local criminal laws relating to computer-related
9 crime;

10 (C) to provide training and education for
11 Federal, State, and local law enforcement per-
12 sonnel regarding investigative technologies and
13 forensic analyses pertaining to computer-related
14 crime;

15 (D) to conduct research and to develop tech-
16 nologies for assistance in investigations and fo-
17 rensic analyses of evidence related to computer-
18 related crimes;

19 (E) to facilitate and promote efficiencies in
20 the sharing of Federal law enforcement expertise,
21 investigative technologies, and forensic analysis
22 pertaining to computer-related crime with State
23 and local law enforcement personnel, prosecutors,
24 regional computer forensic laboratories, and

1 *multijurisdictional computer crime task forces;*
2 *and*

3 *(F) to carry out such other activities as the*
4 *Director considers appropriate.*

5 ***(b) DEVELOPMENT AND SUPPORT OF COMPUTER FO-***
6 ***RENSIC ACTIVITIES.—The Director shall take appropriate***
7 ***actions to develop at least 10 regional computer forensic***
8 ***laboratories, and to provide support, education, and assist-***
9 ***ance for existing computer forensic laboratories, in order***
10 ***that such computer forensic laboratories have the***
11 ***capability—***

12 *(1) to provide forensic examinations with*
13 *respect to seized or intercepted computer evidence*
14 *relating to criminal activity;*

15 *(2) to provide training and education for*
16 *Federal, State, and local law enforcement per-*
17 *sonnel and prosecutors regarding investigations,*
18 *forensic analyses, and prosecutions of computer-*
19 *related crime;*

20 *(3) to assist Federal, State, and local law*
21 *enforcement in enforcing Federal, State, and*
22 *local criminal laws relating to computer-related*
23 *crime;*

24 *(4) to facilitate and promote the sharing of*
25 *Federal law enforcement expertise and informa-*

1 *tion about the investigation, analysis, and pros-*
2 *ecution of computer-related crime with State and*
3 *local law enforcement personnel and prosecutors,*
4 *including the use of multijurisdictional task*
5 *forces; and*

6 *(5) to carry out such other activities as the*
7 *Director considers appropriate.*

8 *(c) AUTHORIZATION OF APPROPRIATIONS.—*

9 *(1) AUTHORIZATION.—There is hereby author-*
10 *ized to be appropriated for fiscal year 2001,*
11 *\$100,000,000 for purposes of carrying out this sec-*
12 *tion, of which \$20,000,000 shall be available solely for*
13 *activities under subsection (b).*

14 *(2) AVAILABILITY.—Amounts appropriated pur-*
15 *suant to the authorization of appropriations in para-*
16 *graph (1) shall remain available until expended.*

Calendar No. 941

106TH CONGRESS
2D SESSION

S. 2448

A BILL

To enhance the protections of the Internet and the critical infrastructure of the United States, and for other purposes.

OCTOBER 5 (legislative day, SEPTEMBER 22), 2000

Reported with an amendment