

Union Calendar No. 160

105TH CONGRESS
1ST Session

H. R. 695

[Report No. 105-108, Parts I, II, III, IV, V]

A BILL

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

SEPTEMBER 29, 1997

Reported from the Committee on Commerce with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

Union Calendar No. 160

105TH CONGRESS
1ST SESSION

H. R. 695

[Report No. 105–108, Parts I, II, III, IV, V]

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 12, 1997

Mr. GOODLATTE (for himself, Ms. LOFGREN, Mr. DELAY, Mr. BOEHNER, Mr. COBLE, Mr. SENSENBRENNER, Mr. BONO, Mr. PEASE, Mr. CANNON, Mr. CONYERS, Mr. BOUCHER, Mr. GEKAS, Mr. SMITH of Texas, Mr. INGLIS of South Carolina, Mr. BRYANT, Mr. CHABOT, Mr. BARR of Georgia, Ms. JACKSON-LEE of Texas, Ms. WATERS, Mr. ACKERMAN, Mr. BAKER, Mr. BARTLETT of Maryland, Mr. CAMPBELL, Mr. CHAMBLISS, Mr. CUNNINGHAM, Mr. DAVIS of Virginia, Mr. DICKEY, Mr. DOOLITTLE, Mr. EHLERS, Mr. ENGEL, Ms. ESHOO, Mr. EVERETT, Mr. EWING, Mr. FARR of California, Mr. GEJDENSON, Mr. GILLMOR, Mr. GOODE, Ms. NORTON, Mr. HORN, Ms. EDDIE BERNICE JOHNSON of Texas, Mr. SAM JOHNSON of Texas, Mr. KOLBE, Mr. MCINTOSH, Mr. McKEON, Mr. MANZULLO, Mr. MATSUI, Mr. MICA, Mr. MINGE, Mr. MOAKLEY, Mr. NETHERCUTT, Mr. PACKARD, Mr. SESSIONS, Mr. UPTON, Mr. WHITE, and Ms. WOOLSEY) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on International Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

MAY 22, 1997

Reported from the Committee on the Judiciary with an amendment

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

Referral to the Committee on International Relations extended for a period
ending not later than July 11, 1997

JUNE 26, 1997

Referral to the Committee on International Relations extended for a period ending not later than July 25, 1997

Referred to the Committees on Commerce, National Security, and the Permanent Select Committee on Intelligence for a period ending not later than September 5, 1997, for consideration of such provisions of the bill and amendment reported by the Committee on the Judiciary as fall within the jurisdiction of those committees pursuant to clause 1(e) and (k), rule X and rule XLVIII, respectively

JULY 25, 1997

Reported from the Committee on the International Relations with an amendment

[Strike out all after the enacting clause and insert the part printed in boldface roman]

JULY 30, 1997

Referral to the Permanent Select Committee on Intelligence extended for a period ending not later than September 12, 1997

JULY 31, 1997

Referral to the Committee on National Security extended for a period ending not later than September 12, 1997

SEPTEMBER 5, 1997

Referral to the Committee on Commerce extended for a period ending not later than September 12, 1997

SEPTEMBER 11, 1997

Referral to the Permanent Select Committee on Intelligence extended for a period ending not later than September 16, 1997

Referral to the Committee on Commerce extended for a period ending not later than September 26, 1997

SEPTEMBER 12, 1997

Reported from the Committee on the National Security with amendments

[Omit the part struck through in bold brackets and insert the part printed in boldface italic and amend the title]

SEPTEMBER 16, 1997

Reported from the Permanent Select Committee on Intelligence with an amendment

[Strike out all after the enacting clause and insert the part printed in boldface roman in double bold brackets]

SEPTEMBER 25, 1997

Referral to the Committee on Commerce extended for a period ending not later than September 29, 1997

SEPTEMBER 29, 1997

Additional sponsors: Mr. HASTINGS of Washington, Mr. COOK, Mr. FOX of

Pennsylvania, Mrs. MORELLA, Mr. BILBRAY, Mrs. MYRICK, Mr. DEFazio, Mr. WATKINS, Mr. FRANKS of New Jersey, Mr. MARTINEZ, Mr. SHAYS, Mr. NADLER, Mr. HOSTETTLER, Mr. FALCONE, Mrs. LINDA SMITH of Washington, Mr. PAXON, Mr. WELDON of Florida, Mr. GORDON, Mr. HUTCHINSON, Ms. RIVERS, Mr. SNOWBARGER, Mrs. TAUSCHER, Mr. DELAHUNT, Mr. ROHRBACHER, Mr. COOKSEY, Mr. MORAN of Virginia, Mr. GALLEGLY, Mr. CAMP, Mr. WEXLER, Mr. WELLER, Mr. SHERMAN, Mr. DREIER, Mr. CALVERT, Mr. CAPPS, Mr. LINDER, Mr. MCINNIS, Mr. GRAHAM, Mr. THOMAS, Ms. MCKINNEY, Ms. MCCARTHY of Missouri, Mr. FRANK of Massachusetts, Mr. SISISKY, Mr. FORBES, Mr. BLUNT, Mr. ISTOOK, Mr. PICKERING, Mr. DOOLEY of California, Mr. LATHAM, Mr. COX of California, Mr. ROEMER, Mr. FAZIO of California, Mr. ADAM SMITH of Washington, Mr. KIND, Mr. BALLENGER, Mr. NEY, Mr. SALMON, Mr. HOUGHTON, Mr. MCHUGH, Ms. FURSE, Mr. HASTINGS of Florida, Mr. DIAZ-BALART, Mr. KING, Ms. SLAUGHTER, Mr. FROST, Mr. BURTON of Indiana, Ms. DUNN, Ms. CHRISTIAN-GREEN, Mr. ENGLISH of Pennsylvania, Mr. LAMPSON, Mr. BRADY, Mr. SMITH of New Jersey, Mrs. CHENOWETH, Mr. COBURN, Mrs. CUBIN, Mr. BOB SCHAEFFER of Colorado, Mr. BARTON of Texas, Mr. LARGENT, Mr. CLEMENT, Mr. HILLIARD, Mr. LUTHER, Mr. CRAPO, Mr. ROGAN, Mr. ANDREWS, Mr. BONILLA, Ms. ROS-LEHTINEN, Mr. GUTKNECHT, Mr. HAYWORTH, Mr. SUNUNU, Mr. SCARBOROUGH, Mr. NEUMANN, Mr. SANFORD, Mr. NORWOOD, Ms. PRYCE of Ohio, Mr. LEWIS of Kentucky, Mr. KASICH, Mr. ARCHER, Mr. HANSEN, Mr. HERGER, Mr. RILEY, Mr. HILL, Mr. TAUZIN, Mr. MORAN of Kansas, Mr. BURR of North Carolina, Mr. BLUMENAUER, Mr. POMEROY, Mr. RIGGS, Mr. KINGSTON, Mr. MILLER of California, Mr. DUNCAN, Mr. WHITFIELD, Mr. SMITH of Oregon, Mr. QUINN, Mr. KENNEDY of Massachusetts, Mrs. KELLY, Mr. METCALF, Mr. MARKEY, Mr. NEAL of Massachusetts, Mrs. EMERSON, Mr. CHRISTENSEN, Mr. WATTS of Oklahoma, Mr. SOUDER, Mr. POMBO, Mr. STENHOLM, Mr. TIAHRT, Mr. MCGOVERN, Mr. PARKER, Mr. WICKER, Mr. BARRETT of Nebraska, Mr. GEPHARDT, Mr. KIM, Mrs. JOHNSON of Connecticut, Mr. LUCAS of Oklahoma, Mr. BROWN of California, Mr. KNOLLENBERG, Mr. TALENT, Mr. TIENEY, Mr. KLUG, Mr. JENKINS, Mr. CONDIT, Mr. HALL of Texas, Mr. BACHUS, Mr. CRANE, Mr. WAMP, Mr. CASTLE, Mr. LAHOOD, Mr. GOODLING, Mr. SHIMKUS, Mr. SERRANO, Mr. HOLDEN, Mr. HOBSON, Mr. RAHALL, Mr. THOMPSON, Mr. THUNE, Mr. CLYBURN, Mr. HILLEARY, Mr. DEAL of Georgia, Mr. COLLINS, Mr. DAN SCHAEFER of Colorado, Mr. HALL of Ohio, Mr. LIVINGSTON, Mr. HOEKSTRA, Mr. WISE, Mr. FILNER, Mr. McDERMOTT, Ms. SANCHEZ, Mrs. THURMAN, Mr. TANNER, Mr. PASTOR, Ms. KAPTUR, Mr. LEWIS of Georgia, Mr. JACKSON of Illinois, Ms. MILLENDER-McDONALD, Mr. CUMMINGS, Mr. JEFFERSON, Mr. FORD, Mr. BARRETT of Wisconsin, Mr. FATTAH, Mr. BARCIA, Ms. HOOLEY of Oregon, Mrs. NORTHUP, Mr. VENTO, Mr. BONIOR, Mrs. CLAYTON, Mrs. KENNELLY of Connecticut, Mr. PALLONE, Mr. OLVER, Ms. KILPATRICK, Ms. DELAURO, Mrs. MEEK of Florida, Ms. STABENOW, Mr. STEARNS, Mr. RADANOVICH, Mr. TAYLOR of North Carolina, Mr. WALSH, Mr. NUSSLE, Mr. DAVIS of Illinois, and Mr. RUSH

Deleted sponsors: Mr. EVERETT (added February 12, 1997; deleted July 30,

1997), Ms. EDDIE BERNICE JOHNSON of Texas (added February 12, 1997; deleted May 13, 1997), Mr. SOLOMON (added March 13, 1997; deleted April 29, 1997), Mr. ROTHMAN (added April 10, 1997; deleted July 24, 1997), Mr. JONES (added June 23, 1997; deleted September 8, 1997), Mr. BUNNING (added July 9, 1997; deleted July 30, 1997), Mr. THORNBERRY (added July 24, 1997; deleted September 4, 1997), and Mr. HEFLEY (added July 29, 1997; deleted July 30, 1997)

SEPTEMBER 29, 1997

Reported from the Committee on Commerce with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in boldface italic in bold parentheses]

A BILL

To amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.

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.**

4 This Act may be cited as the “Security and Freedom
 5 Through Encryption (SAFE) Act”.

6 **SEC. 2. SALE AND USE OF ENCRYPTION.**

7 (a) ~~IN GENERAL.~~—Part I of title 18, United States
 8 Code, is amended by inserting after chapter 121 the fol-
 9 lowing new chapter:

10 **“CHAPTER 122—ENCRYPTED WIRE AND**
 11 **ELECTRONIC INFORMATION**

“2801. Definitions:

“2802. Freedom to use encryption:

“2803. Freedom to sell encryption.

“2804. Prohibition on mandatory key escrow.

“2805. Unlawful use of encryption in furtherance of a criminal act.

1 **“§ 2801. Definitions**

2 “As used in this chapter—

3 “(1) the terms ‘person’, ‘State’, ‘wire commu-
4 nication’, ‘electronic communication’, ‘investigative
5 or law enforcement officer’, ‘judge of competent ju-
6 risdiction’, and ‘electronic storage’ have the mean-
7 ings given those terms in section 2510 of this title;

8 “(2) the terms ‘encrypt’ and ‘encryption’ refer
9 to the scrambling of wire or electronic information
10 using mathematical formulas or algorithms in order
11 to preserve the confidentiality, integrity, or authen-
12 ticity of, and prevent unauthorized recipients from
13 accessing or altering, such information;

14 “(3) the term ‘key’ means the variable informa-
15 tion used in a mathematical formula, code, or algo-
16 rithm, or any component thereof, used to decrypt
17 wire or electronic information that has been
18 encrypted; and

19 “(4) the term ‘United States person’ means—

20 “(A) any United States citizen;

21 “(B) any other person organized under the
22 laws of any State, the District of Columbia, or
23 any commonwealth, territory, or possession of
24 the United States; and

1 “(C) any person organized under the laws
2 of any foreign country who is owned or con-
3 trolled by individuals or persons described in
4 subparagraphs (A) and (B).

5 **“§ 2802. Freedom to use eneryption**

6 “Subject to section 2805, it shall be lawful for any
7 person within any State, and for any United States person
8 in a foreign country, to use any eneryption, regardless of
9 the eneryption algorithm selected, eneryption key length
10 chosen, or implementation technique or medium used.

11 **“§ 2803. Freedom to sell eneryption**

12 “Subject to section 2805, it shall be lawful for any
13 person within any State to sell in interstate commerce any
14 eneryption, regardless of the eneryption algorithm se-
15 lected, eneryption key length chosen, or implementation
16 technique or medium used.

17 **“§ 2804. Prohibition on mandatory key escrow**

18 “(a) PROHIBITION.—No person in lawful possession
19 of a key to encrypted information may be required by Fed-
20 eral or State law to relinquish to another person control
21 of that key.

22 “(b) EXCEPTION FOR ACCESS FOR LAW ENFORCE-
23 MENT PURPOSES.—Subsection (a) shall not affect the au-
24 thority of any investigative or law enforcement officer, act-

ing under any law in effect on the effective date of this chapter, to gain access to encrypted information.

“§ 2805. Unlawful use of eneryption in furtherance of a criminal act

“Any person who willfully uses eneryption in furtherance of the commission of a criminal offense for which the person may be prosecuted in a court of competent jurisdiction—

“(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined in the amount set forth in this title, or both; and

“(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined in the amount set forth in this title, or both.”

(b) CONFORMING AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 33 the following new item:

“122. Encrypted wire and electronic information 2801”.

[SEC. 3. EXPORTS OF ENCRYPTION.

[(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF 1979.—Section 17 of the Export Administration Act of 1979 (50 U.S.C. App. 2416) is amended by adding at the end thereof the following new subsection:

1 ~~“(g) COMPUTERS AND RELATED EQUIPMENT.—~~

2 ~~“(1) GENERAL RULE.—Subject to paragraphs~~
 3 ~~(2), (3), and (4), the Secretary shall have exclusive~~
 4 ~~authority to control exports of all computer hard-~~
 5 ~~ware, software, and technology for information secu-~~
 6 ~~rity (including encryption), except that which is spe-~~
 7 ~~cifically designed or modified for military use, in-~~
 8 ~~cluding command, control, and intelligence applica-~~
 9 ~~tions.~~

10 ~~“(2) ITEMS NOT REQUIRING LICENSES.—No~~
 11 ~~validated license may be required, except pursuant~~
 12 ~~to the Trading With The Enemy Act or the Inter-~~
 13 ~~national Emergency Economic Powers Act (but only~~
 14 ~~to the extent that the authority of such Act is not~~
 15 ~~exercised to extend controls imposed under this Act),~~
 16 ~~for the export or reexport of—~~

17 ~~“(A) any software, including software~~
 18 ~~with encryption capabilities—~~

19 ~~“(i) that is generally available, as is,~~
 20 ~~and is designed for installation by the pur-~~
 21 ~~chaser; or~~

22 ~~“(ii) that is in the public domain for~~
 23 ~~which copyright or other protection is not~~
 24 ~~available under title 17, United States~~
 25 ~~Code, or that is available to the public be-~~

cause it is generally accessible to the interested public in any form; or

~~“(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).~~

~~“(3) SOFTWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of software with encryption capabilities for nonmilitary end uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be—~~

~~“(A) diverted to a military end use or an end use supporting international terrorism;~~

~~“(B) modified for military or terrorist end use; or~~

~~“(C) reexported without any authorization by the United States that may be required under this Act.~~

~~“(4) HARDWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of computer hardware with encryption ca-~~

1 pabilities if the Secretary determines that a product
2 offering comparable security is commercially avail-
3 able outside the United States from a foreign sup-
4 plier, without effective restrictions.

5 ¶“(5) DEFINITIONS.—As used in this sub-
6 section—

7 ¶“(A) the term ‘encryption’ means the
8 scrambling of wire or electronic information
9 using mathematical formulas or algorithms in
10 order to preserve the confidentiality, integrity,
11 or authenticity of, and prevent unauthorized re-
12 cipients from accessing or altering, such infor-
13 mation;

14 ¶“(B) the term ‘generally available’ means,
15 in the case of software (including software with
16 encryption capabilities), software that is offered
17 for sale, license, or transfer to any person with-
18 out restriction, whether or not for consider-
19 ation, including, but not limited to, over-the-
20 counter retail sales, mail order transactions,
21 phone order transactions, electronic distribu-
22 tion, or sale on approval;

23 ¶“(C) the term ‘as is’ means, in the case
24 of software (including software with encryption
25 capabilities), a software program that is not de-

1 signed, developed, or tailored by the software
2 publisher for specific purchasers, except that
3 such purchasers may supply certain installation
4 parameters needed by the software program to
5 function properly with the purchaser's system
6 and may customize the software program by
7 choosing among options contained in the soft-
8 ware program;

9 ¶“(D) the term ‘is designed for installation
10 by the purchaser’ means, in the case of soft-
11 ware (including software with encryption capa-
12 bilities) that—

13 ¶“(i) the software publisher intends
14 for the purchaser (including any licensee or
15 transferee), who may not be the actual
16 program user, to install the software pro-
17 gram on a computing device and has sup-
18 plied the necessary instructions to do so,
19 except that the publisher may also provide
20 telephone help line services for software in-
21 stallation, electronic transmission, or basic
22 operations; and

23 ¶“(ii) the software program is de-
24 signed for installation by the purchaser

1 without further substantial support by the
2 supplier;

3 ~~“(E) the term ‘computing device’ means~~
4 ~~a device which incorporates one or more micro-~~
5 ~~processor-based central processing units that~~
6 ~~can accept, store, process, or provide output of~~
7 ~~data; and~~

8 ~~“(F) the term ‘computer hardware’, when~~
9 ~~used in conjunction with information security,~~
10 ~~includes, but is not limited to, computer sys-~~
11 ~~tems, equipment, application-specific assem-~~
12 ~~blies, modules, and integrated circuits.”.~~

13 ~~[(b) CONTINUATION OF EXPORT ADMINISTRATION~~
14 ~~ACT.—For purposes of carrying out the amendment made~~
15 ~~by subsection (a), the Export Administration Act of 1979~~
16 ~~shall be deemed to be in effect.]~~

17 **SEC. 3. EXPORTS OF ENCRYPTION.**

18 **(a) EXPORT CONTROL OF ENCRYPTION PROD-**
19 **UCTS NOT CONTROLLED ON THE UNITED STATES**
20 **MUNITIONS LIST.—The Secretary of Commerce,**
21 **with the concurrence of the Secretary of De-**
22 **fense, shall have the authority to control the**
23 **export of encryption products not controlled**
24 **on the United States Munitions List. Decisions**
25 **made by the Secretary of Commerce with the**

1 *concurrence of the Secretary of Defense with*
2 *respect to exports of encryption products*
3 *under this section shall not be subject to judi-*
4 *cial review.*

5 **(b) LICENSE EXCEPTION FOR CERTAIN**
6 **ENCRYPTION PRODUCTS.**—*Encryption products*
7 *with encryption strength equal to or less than*
8 *the level identified in subsection (d) shall be*
9 *eligible for export under a license exception*
10 *after a 1-time review, if the encryption product*
11 *being exported does not include features that*
12 *would otherwise require licensing under ap-*
13 *plicable regulations, is not destined for coun-*
14 *tries, end-users, or end-uses that the Secretary*
15 *of Commerce has determined by regulation,*
16 *with the concurrence of the Secretary of De-*
17 *fense, are ineligible to receive such products,*
18 *and is otherwise qualified for export.*

19 **(c) ONE-TIME PRODUCT REVIEW.**—*The Sec-*
20 *retary of Commerce, with the concurrence of*
21 *the Secretary of Defense, shall specify the in-*
22 *formation that must be submitted for the 1-*
23 *time review referred to in subsection (b).*

24 **(d) ELIGIBLE ENCRYPTION LEVELS.**—

1 **(1) INITIAL ELIGIBILITY LEVEL.—***Not*
2 *later than 30 days after the date of the en-*
3 *actment of this Act, the President shall*
4 *notify the Congress of the maximum level*
5 *of encryption strength that could be ex-*
6 *ported from the United States under li-*
7 *cense exception pursuant to this section*
8 *without harm to the national security of*
9 *the United States. Such level shall not be-*
10 *come effective until 60 days after such no-*
11 *tification.*

12 **(2) ANNUAL REVIEW OF ELIGIBILITY**
13 **LEVEL.—***Not later than 1 year after notify-*
14 *ing the Congress of the maximum level of*
15 *encryption strength under paragraph (1),*
16 *and annually thereafter, the President*
17 *shall notify the Congress of the maximum*
18 *level of encryption strength that could be*
19 *exported from the United States under li-*
20 *cense exception pursuant to this section*
21 *without harm to the national security of*
22 *the United States. Such level shall not be-*
23 *come effective until 60 days after such no-*
24 *tification.*

1 **(3) CALCULATION OF 60-DAY PERIOD.—**

2 *The 60-day period referred to in para-*
 3 *graphs (1) and (2) shall be computed by*
 4 *excluding—*

5 **(A) the days on which either**
 6 **House is not in session because of an**
 7 **adjournment of more than 3 days to a**
 8 **day certain or an adjournment of the**
 9 **Congress sine die; and**

10 **(B) each Saturday and Sunday,**
 11 **not excluded under subparagraph (A),**
 12 **when either House is not in session.**

13 **(e) EXERCISE OF EXISTING AUTHORITIES.—**

14 *The Secretary of Commerce and the Secretary*
 15 *of Defense may exercise the authorities they*
 16 *have under other provisions of law to carry out*
 17 *this section.*

18 **SECTION 1. SHORT TITLE.**

19 *This Act may be cited as the “Security and Freedom*
 20 *Through Encryption (SAFE) Act”.*

21 **SEC. 2. SALE AND USE OF ENCRYPTION.**

22 **(a) IN GENERAL.—***Part I of title 18, United States*
 23 *Code, is amended by inserting after chapter 123 the follow-*
 24 *ing new chapter:*

1 **“CHAPTER 125—ENCRYPTED WIRE AND**
 2 **ELECTRONIC INFORMATION**

“2801. Definitions.

“2802. Freedom to use encryption.

“2803. Freedom to sell encryption.

“2804. Prohibition on mandatory key escrow.

“2805. Unlawful use of encryption in furtherance of a criminal act.

3 **“§2801. Definitions**

4 *“As used in this chapter—*

5 *“(1) the terms ‘person’, ‘State’, ‘wire commu-*
 6 *nication’, ‘electronic communication’, ‘investigative or*
 7 *law enforcement officer’, and ‘judge of competent ju-*
 8 *risdiction’ have the meanings given those terms in*
 9 *section 2510 of this title;*

10 *“(2) the terms ‘encrypt’ and ‘encryption’ refer to*
 11 *the scrambling of wire communications, electronic*
 12 *communications, or electronically stored information,*
 13 *using mathematical formulas or algorithms in order*
 14 *to preserve the confidentiality, integrity, or authentic-*
 15 *ity of, and prevent unauthorized recipients from*
 16 *accessing or altering, such communications or infor-*
 17 *mation;*

18 *“(3) the term ‘key’ means the variable informa-*
 19 *tion used in a mathematical formula, code, or algo-*
 20 *rithm, or any component thereof, used to decrypt wire*
 21 *communications, electronic communications, or elec-*
 22 *tronically stored information, that has been*
 23 *encrypted; and*

1 “(4) the term ‘United States person’ means—

2 “(A) any United States citizen;

3 “(B) any other person organized under the
4 laws of any State, the District of Columbia, or
5 any commonwealth, territory, or possession of
6 the United States; and

7 “(C) any person organized under the laws
8 of any foreign country who is owned or con-
9 trolled by individuals or persons described in
10 subparagraphs (A) and (B).

11 **“§ 2802. Freedom to use encryption**

12 “Subject to section 2805, it shall be lawful for any per-
13 son within any State, and for any United States person
14 in a foreign country, to use any encryption, regardless of
15 the encryption algorithm selected, encryption key length
16 chosen, or implementation technique or medium used.

17 **“§ 2803. Freedom to sell encryption**

18 “Subject to section 2805, it shall be lawful for any per-
19 son within any State to sell in interstate commerce any
20 encryption, regardless of the encryption algorithm selected,
21 encryption key length chosen, or implementation technique
22 or medium used.

23 **“§ 2804. Prohibition on mandatory key escrow**

24 “(a) PROHIBITION.—No person in lawful possession of
25 a key to encrypted communications or information may be

1 *required by Federal or State law to relinquish to another*
 2 *person control of that key.*

3 “(b) *EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT*
 4 *PURPOSES.*—Subsection (a) shall not affect the authority
 5 of any investigative or law enforcement officer, or any
 6 member of the intelligence community as defined in section
 7 3 of the National Security Act of 1947 (50 U.S.C. 401a),
 8 acting under any law in effect on the effective date of this
 9 chapter, to gain access to encrypted communications or in-
 10 formation.

11 **“§2805. Unlawful use of encryption in furtherance of**
 12 **a criminal act**

13 “Any person who, in the commission of a felony under
 14 a criminal statute of the United States, knowingly and will-
 15 fully encrypts incriminating communications or informa-
 16 tion relating to that felony with the intent to conceal such
 17 communications or information for the purpose of avoiding
 18 detection by law enforcement agencies or prosecution—

19 “(1) in the case of a first offense under this sec-
 20 tion, shall be imprisoned for not more than 5 years,
 21 or fined in the amount set forth in this title, or both;
 22 and

23 “(2) in the case of a second or subsequent offense
 24 under this section, shall be imprisoned for not more

1 *than 10 years, or fined in the amount set forth in this*
 2 *title, or both.”.*

3 (b) *CONFORMING AMENDMENT.*—*The table of chapters*
 4 *for part I of title 18, United States Code, is amended by*
 5 *inserting after the item relating to chapter 123 the following*
 6 *new item:*

“125. *Encrypted wire and electronic information* 2801”.

7 **SEC. 3. *EXPORTS OF ENCRYPTION.***

8 (a) *AMENDMENT TO EXPORT ADMINISTRATION ACT OF*
 9 *1979.*—*Section 17 of the Export Administration Act of*
 10 *1979 (50 U.S.C. App. 2416) is amended by adding at the*
 11 *end thereof the following new subsection:*

12 “(g) *COMPUTERS AND RELATED EQUIPMENT.*—

13 “(1) *GENERAL RULE.*—*Subject to paragraphs*
 14 *(2), (3), and (4), the Secretary shall have exclusive*
 15 *authority to control exports of all computer hardware,*
 16 *software, and technology for information security (in-*
 17 *cluding encryption), except that which is specifically*
 18 *designed or modified for military use, including com-*
 19 *mand, control, and intelligence applications.*

20 “(2) *ITEMS NOT REQUIRING LICENSES.*—*No vali-*
 21 *dated license may be required, except pursuant to the*
 22 *Trading With The Enemy Act or the International*
 23 *Emergency Economic Powers Act (but only to the ex-*
 24 *tent that the authority of such Act is not exercised to*

1 *extend controls imposed under this Act), for the export*
2 *or reexport of—*

3 “(A) *any software, including software with*
4 *encryption capabilities—*

5 “(i) *that is generally available, as is,*
6 *and is designed for installation by the pur-*
7 *chaser; or*

8 “(ii) *that is in the public domain for*
9 *which copyright or other protection is not*
10 *available under title 17, United States*
11 *Code, or that is available to the public be-*
12 *cause it is generally accessible to the inter-*
13 *ested public in any form; or*

14 “(B) *any computing device solely because it*
15 *incorporates or employs in any form software*
16 *(including software with encryption capabilities)*
17 *exempted from any requirement for a validated*
18 *license under subparagraph (A).*

19 “(3) *SOFTWARE WITH ENCRYPTION CAPABILI-*
20 *TIES.—The Secretary shall authorize the export or re-*
21 *export of software with encryption capabilities for*
22 *nonmilitary end uses in any country to which exports*
23 *of software of similar capability are permitted for use*
24 *by financial institutions not controlled in fact by*

1 *United States persons, unless there is substantial evi-*
2 *dence that such software will be—*

3 *“(A) diverted to a military end use or an*
4 *end use supporting international terrorism;*

5 *“(B) modified for military or terrorist end*
6 *use; or*

7 *“(C) reexported without any authorization*
8 *by the United States that may be required under*
9 *this Act.*

10 *“(4) HARDWARE WITH ENCRYPTION CAPABILI-*
11 *TIES.—The Secretary shall authorize the export or re-*
12 *export of computer hardware with encryption capa-*
13 *bilities if the Secretary determines that a product of-*
14 *fering comparable security is commercially available*
15 *outside the United States from a foreign supplier,*
16 *without effective restrictions.*

17 *“(5) DEFINITIONS.—As used in this subsection—*

18 *“(A) the term ‘encryption’ means the scram-*
19 *bling of wire or electronic information using*
20 *mathematical formulas or algorithms in order to*
21 *preserve the confidentiality, integrity, or authen-*
22 *ticity of, and prevent unauthorized recipients*
23 *from accessing or altering, such information;*

24 *“(B) the term ‘generally available’ means,*
25 *in the case of software (including software with*

1 *encryption capabilities), software that is offered*
2 *for sale, license, or transfer to any person with-*
3 *out restriction, whether or not for consideration,*
4 *including, but not limited to, over-the-counter re-*
5 *tail sales, mail order transactions, phone order*
6 *transactions, electronic distribution, or sale on*
7 *approval;*

8 *“(C) the term ‘as is’ means, in the case of*
9 *software (including software with encryption ca-*
10 *pabilities), a software program that is not de-*
11 *signed, developed, or tailored by the software*
12 *publisher for specific purchasers, except that such*
13 *purchasers may supply certain installation pa-*
14 *rameters needed by the software program to*
15 *function properly with the purchaser’s system*
16 *and may customize the software program by*
17 *choosing among options contained in the soft-*
18 *ware program;*

19 *“(D) the term ‘is designed for installation*
20 *by the purchaser’ means, in the case of software*
21 *(including software with encryption capabilities)*
22 *that—*

23 *“(i) the software publisher intends for*
24 *the purchaser (including any licensee or*
25 *transferee), who may not be the actual pro-*

1 *gram user, to install the software program*
 2 *on a computing device and has supplied the*
 3 *necessary instructions to do so, except that*
 4 *the publisher may also provide telephone*
 5 *help line services for software installation,*
 6 *electronic transmission, or basic operations;*
 7 *and*

8 *“(ii) the software program is designed*
 9 *for installation by the purchaser without*
 10 *further substantial support by the supplier;*

11 *“(E) the term ‘computing device’ means a*
 12 *device which incorporates one or more micro-*
 13 *processor-based central processing units that can*
 14 *accept, store, process, or provide output of data;*
 15 *and*

16 *“(F) the term ‘computer hardware’, when*
 17 *used in conjunction with information security,*
 18 *includes, but is not limited to, computer systems,*
 19 *equipment, application-specific assemblies, mod-*
 20 *ules, and integrated circuits.”.*

21 *(b) CONTINUATION OF EXPORT ADMINISTRATION*

22 *ACT.—For purposes of carrying out the amendment made*
 23 *by subsection (a), the Export Administration Act of 1979*
 24 *shall be deemed to be in effect.*

1 **SEC. 4. EFFECT ON LAW ENFORCEMENT ACTIVITIES.**

2 (a) *COLLECTION OF INFORMATION BY ATTORNEY GEN-*
 3 *ERAL.—The Attorney General shall compile, and maintain*
 4 *in classified form, data on the instances in which*
 5 *encryption (as defined in section 2801 of title 18, United*
 6 *States Code) has interfered with, impeded, or obstructed the*
 7 *ability of the Department of Justice to enforce the criminal*
 8 *laws of the United States.*

9 (b) *AVAILABILITY OF INFORMATION TO THE CON-*
 10 *GRESS.—The information compiled under subsection (a),*
 11 *including an unclassified summary thereof, shall be made*
 12 *available, upon request, to any Member of Congress.*

13 **SECTION 1. SHORT TITLE.**

14 **This Act may be cited as the “Security and**
 15 **Freedom Through Encryption (SAFE) Act”.**

16 **SEC. 2. SALE AND USE OF ENCRYPTION.**

17 **(a) IN GENERAL.—Part I of title 18, United**
 18 **States Code, is amended by inserting after**
 19 **chapter 121 the following new chapter:**

20 **“CHAPTER 122—ENCRYPTED WIRE AND**
 21 **ELECTRONIC INFORMATION**

“2801. Definitions.

“2802. Freedom to use encryption.

“2803. Freedom to sell encryption.

“2804. Prohibition on mandatory key escrow.

“2805. Unlawful use of encryption in furtherance of a criminal
 act.

1 **“§ 2801. Definitions**

2 **“As used in this chapter—**

3 **“(1) the terms ‘person’, ‘State’, ‘wire**
4 **communication’, ‘electronic communica-**
5 **tion’, ‘investigative or law enforcement**
6 **officer’, ‘judge of competent jurisdiction’,**
7 **and ‘electronic storage’ have the mean-**
8 **ings given those terms in section 2510 of**
9 **this title;**

10 **“(2) the terms ‘encrypt’ and**
11 **‘encryption’ refer to the scrambling of**
12 **wire or electronic information using**
13 **mathematical formulas or algorithms in**
14 **order to preserve the confidentiality, in-**
15 **tegrity, or authenticity of, and prevent**
16 **unauthorized recipients from accessing**
17 **or altering, such information;**

18 **“(3) the term ‘key’ means the variable**
19 **information used in a mathematical for-**
20 **mula, code, or algorithm, or any compo-**
21 **nent thereof, used to decrypt wire or**
22 **electronic information that has been**
23 **encrypted; and**

24 **“(4) the term ‘United States person’**
25 **means—**

26 **“(A) any United States citizen;**

1 “(B) any other person organized
2 under the laws of any State, the Dis-
3 trict of Columbia, or any common-
4 wealth, territory, or possession of the
5 United States; and

6 “(C) any person organized under
7 the laws of any foreign country who
8 is owned or controlled by individuals
9 or persons described in subpara-
10 graphs (A) and (B).

11 “§ 2802. Freedom to use encryption

12 “Subject to section 2805, it shall be lawful
13 for any person within any State, and for any
14 United States person in a foreign country, to
15 use any encryption, regardless of the
16 encryption algorithm selected, encryption
17 key length chosen, or implementation tech-
18 nique or medium used.

19 “§ 2803. Freedom to sell encryption

20 “Subject to section 2805, it shall be lawful
21 for any person within any State to sell in
22 interstate commerce any encryption, regard-
23 less of the encryption algorithm selected,
24 encryption key length chosen, or implementa-
25 tion technique or medium used.

1 **“§ 2804. Prohibition on mandatory key escrow**

2 **“(a) PROHIBITION.—No person in lawful**
3 **possession of a key to encrypted information**
4 **may be required by Federal or State law to re-**
5 **linquish to another person control of that key.**

6 **“(b) EXCEPTION FOR ACCESS FOR LAW EN-**
7 **FORCEMENT PURPOSES.—Subsection (a) shall**
8 **not affect the authority of any investigative or**
9 **law enforcement officer, acting under any law**
10 **in effect on the effective date of this chapter,**
11 **to gain access to encrypted information.**

12 **“§ 2805. Unlawful use of encryption in furtherance of**
13 **a criminal act**

14 **“Any person who willfully uses encryption**
15 **in furtherance of the commission of a crimi-**
16 **nal offense for which the person may be pros-**
17 **ecuted in a court of competent jurisdiction—**

18 **“(1) in the case of a first offense**
19 **under this section, shall be imprisoned**
20 **for not more than 5 years, or fined in the**
21 **amount set forth in this title, or both; and**

22 **“(2) in the case of a second or subse-**
23 **quent offense under this section, shall be**
24 **imprisoned for not more than 10 years, or**
25 **fined in the amount set forth in this title,**
26 **or both.”.**

1 **(b) CONFORMING AMENDMENT.—The table of**
 2 **chapters for part I of title 18, United States**
 3 **Code, is amended by inserting after the item**
 4 **relating to chapter 33 the following new item:**

“122. Encrypted wire and electronic information 2801”.

5 **SEC. 3. EXPORTS OF ENCRYPTION.**

6 **(a) AMENDMENT TO EXPORT ADMINISTRATION**
 7 **ACT OF 1979.—Section 17 of the Export Admin-**
 8 **istration Act of 1979 (50 U.S.C. App. 2416) is**
 9 **amended by adding at the end thereof the fol-**
 10 **lowing new subsection:**

11 **“(g) CERTAIN CONSUMER PRODUCTS, COM-**
 12 **PUTERS, AND RELATED EQUIPMENT.—**

13 **“(1) GENERAL RULE.—Subject to para-**
 14 **graphs (2), (3), and (4), the Secretary shall**
 15 **have exclusive authority to control ex-**
 16 **ports of all computer hardware, software,**
 17 **and technology for information security**
 18 **(including encryption), except that which**
 19 **is specifically designed or modified for**
 20 **military use, including command, control,**
 21 **and intelligence applications.**

22 **“(2) ITEMS NOT REQUIRING LICENSES.—**
 23 **No validated license may be required, ex-**
 24 **cept pursuant to the Trading With The**
 25 **Enemy Act or the International Emer-**

1 **gency Economic Powers Act (but only to**
2 **the extent that the authority of such Act**
3 **is not exercised to extend controls im-**
4 **posed under this Act), for the export or**
5 **reexport of—**

6 **“(A) any consumer product com-**
7 **mercially available within the United**
8 **States or abroad which—**

9 **“(i) includes encryption capa-**
10 **bilities which are inaccessible to**
11 **the end user; and**

12 **“(ii) is not designed for mili-**
13 **tary or intelligence end use;**

14 **“(B) any component or subassem-**
15 **bly designed for use in a consumer**
16 **product described in subparagraph**
17 **(A) which itself contains encryption**
18 **capabilities and is not capable of mili-**
19 **tary or intelligence end use in its con-**
20 **dition as exported;**

21 **“(C) any software, including soft-**
22 **ware with encryption capabilities—**

23 **“(i) that is generally available,**
24 **as is, and is designed for installa-**
25 **tion by the purchaser;**

1 “(ii) that is in the public do-
2 main for which copyright or other
3 protection is not available under
4 title 17, United States Code, or
5 that is available to the public be-
6 cause it is generally accessible to
7 the interested public in any form;
8 or

9 “(iii) that is customized for an
10 otherwise lawful use by a specific
11 purchaser or group of purchasers;

12 “(D) any computing device solely
13 because it incorporates or employs in
14 any form—

15 “(i) software (including soft-
16 ware with encryption capabili-
17 ties) that is exempted from any
18 requirement for a validated li-
19 cense under subparagraph (C); or

20 “(ii) software that is no more
21 technically complex in its
22 encryption capabilities than soft-
23 ware that is exempted from any
24 requirement for a validated li-
25 cense under subparagraph (C) but

1 is not designed for installation by
2 the purchaser;

3 “(E) any computer hardware that
4 is generally available, solely because
5 it has encryption capabilities; or

6 “(F) any software or computing
7 device solely on the basis that it in-
8 corporates or employs in any form
9 interface mechanisms for interaction
10 with other hardware and software,
11 including hardware, and software,
12 with encryption capabilities.

13 “(3) SOFTWARE WITH ENCRYPTION CAPA-
14 BILITIES.—The Secretary shall authorize
15 the export or reexport of software with
16 encryption capabilities for nonmilitary
17 end uses in any country to which exports
18 of software of similar capability are per-
19 mitted for use by financial institutions
20 not controlled in fact by United States
21 persons, unless there is substantial evi-
22 dence that such software will be—

23 “(A) diverted to a military end use
24 or an end use supporting inter-
25 national terrorism;

1 “(B) modified for military or ter-
2 rorist end use; or

3 “(C) reexported without any au-
4 thorization by the United States that
5 may be required under this Act.

6 “(4) **HARDWARE WITH ENCRYPTION CAPA-**
7 **BILITIES.—**The Secretary shall authorize
8 the export or reexport of computer hard-
9 ware with encryption capabilities if the
10 Secretary determines that a product of-
11 fering comparable security is commer-
12 cially available outside the United States
13 from a foreign supplier, without effective
14 restrictions.

15 “(5) **DEFINITIONS.—**As used in this sub-
16 section—

17 “(A) the term ‘encryption’ means
18 the scrambling of wire or electronic
19 information using mathematical for-
20 mulas or algorithms in order to pre-
21 serve the confidentiality, integrity, or
22 authenticity of, and prevent unau-
23 thorized recipients from accessing or
24 altering, such information;

1 **“(B) the term ‘generally available’**
2 **means—**

3 **“(i) in the case of software (in-**
4 **cluding software with encryption**
5 **capabilities), software that is of-**
6 **fered for sale, license, or transfer**
7 **to any person without restriction,**
8 **whether or not for consideration,**
9 **including, but not limited to,**
10 **over-the-counter retail sales, mail**
11 **order transactions, phone order**
12 **transactions, electronic distribu-**
13 **tion, or sale on approval; and**

14 **“(ii) in the case of hardware**
15 **with encryption capabilities,**
16 **hardware that is offered for sale,**
17 **license, or transfer to any person**
18 **without restriction, whether or**
19 **not for consideration, including,**
20 **but not limited to, over-the-**
21 **counter retail sales, mail order**
22 **transactions, phone order trans-**
23 **actions, electronic distribution, or**
24 **sale on approval;**

1 “(C) the term ‘as is’ means, in the
2 case of software (including software
3 with encryption capabilities), a soft-
4 ware program that is not designed,
5 developed, or tailored by the software
6 publisher for specific purchasers, ex-
7 cept that such purchasers may supply
8 certain installation parameters need-
9 ed by the software program to func-
10 tion properly with the purchaser’s
11 system and may customize the soft-
12 ware program by choosing among op-
13 tions contained in the software pro-
14 gram;

15 “(D) the term ‘is designed for in-
16 stallation by the purchaser’ means, in
17 the case of software (including soft-
18 ware with encryption capabilities)
19 that—

20 “(i) the software publisher in-
21 tends for the purchaser (includ-
22 ing any licensee or transferee),
23 who may not be the actual pro-
24 gram user, to install the software
25 program on a computing device

1 and has supplied the necessary
2 instructions to do so, except that
3 the publisher may also provide
4 telephone help line services for
5 software installation, electronic
6 transmission, or basic operations;
7 and

8 “(ii) the software program is
9 designed for installation by the
10 purchaser without further sub-
11 stantial support by the supplier;

12 “(E) the term ‘computing device’
13 means a device which incorporates
14 one or more microprocessor-based
15 central processing units that can ac-
16 cept, store, process, or provide output
17 of data; and

18 “(F) the term ‘computer hard-
19 ware’, when used in conjunction with
20 information security, includes, but is
21 not limited to, computer systems,
22 equipment, application-specific as-
23 semblies, modules, and integrated cir-
24 cuits.”.

1 **(b) CONTINUATION OF EXPORT ADMINISTRA-**
2 **TION ACT.—For purposes of carrying out the**
3 **amendment made by subsection (a), the Ex-**
4 **port Administration Act of 1979 shall be**
5 **deemed to be in effect.**

6 **SEC. 4. SENSE OF CONGRESS REGARDING INTERNATIONAL**
7 **COOPERATION.**

8 **(a) FINDINGS.—The Congress finds that—**

9 **(1) implementing export restrictions**
10 **on widely available technology without**
11 **the concurrence of all countries capable**
12 **of producing, transshipping, or otherwise**
13 **transferring that technology is detrimen-**
14 **tal to the competitiveness of the United**
15 **States and should only be imposed on**
16 **technology and countries in order to pro-**
17 **tect the United States against a compel-**
18 **ling national security threat; and**

19 **(2) the President has not been able to**
20 **come to agreement with other encryption**
21 **producing countries on export controls**
22 **on encryption and has imposed exces-**
23 **sively stringent export controls on this**
24 **widely available technology.**

10 **[(a) SHORT TITLE.—This Act may be cited**
11 **as the “Security and Freedom through**
12 **Encryption (“SAFE”) Act of 1997”.**

[[Sec. 2. Statement of policy.

[[Sec. 104. Unlawful use of encryption.

[[Sec. 206. Implementation.

- [[Sec. 303. License exception for telecommunications products.**
- [[Sec. 304. Review for certain institutions.**
- [[Sec. 305. Encryption industry and information security board.**

[[TITLE IV—LIABILITY LIMITATIONS

- [[Sec. 401. Compliance with court order.**
- [[Sec. 402. Compliance defense.**
- [[Sec. 403. Reasonable care defense.**
- [[Sec. 404. Good faith defense.**
- [[Sec. 405. Sovereign immunity.**
- [[Sec. 406. Civil action, generally.**

[[TITLE V—INTERNATIONAL AGREEMENTS

- [[Sec. 501. Sense of congress.**
- [[Sec. 502. Failure to negotiate.**
- [[Sec. 503. Report to congress.**

[[TITLE VI—MISCELLANEOUS PROVISIONS

- [[Sec. 601. Effect on law enforcement activities.**
- [[Sec. 602. Interpretation.**
- [[Sec. 603. Severability.**

1 [[SEC. 2. STATEMENT OF POLICY.

2 **[[It is the policy of the United States to**
 3 **protect public computer networks through**
 4 **the use of strong encryption technology, to**
 5 **promote and improve the export of**
 6 **encryption products developed and manufac-**
 7 **tured in the United States, and to preserve**
 8 **public safety and national security.**

9 [[TITLE I—DOMESTIC USES OF 10 **ENCRYPTION**

11 [[SEC. 101. DEFINITIONS.

12 **[[For purposes of this Act:**

13 **[[(1) ATTORNEY FOR THE GOVERN-**
 14 **MENT.—The term “attorney for the Gov-**

1 ernment” has the meaning given such
2 term in Rule 54(c) of the Federal Rules of
3 Criminal Procedure, and also includes
4 any duly authorized attorney of a State
5 who is authorized to prosecute criminal
6 offenses within such State.

7 **[(2) CERTIFICATE AUTHORITY.—**The
8 term “certificate authority” means a per-
9 son trusted by one or more persons to
10 create and assign public key certificates.

11 **[(3) COMMUNICATIONS.—**The term
12 “communications” means any wire com-
13 munications or electronic communica-
14 tions as those terms are defined in para-
15 graphs (1) and (12) of section 2510 of title
16 18, United States Code.

17 **[(4) COURT OF COMPETENT JURISDIC-**
18 **TION.—**The term “court of competent ju-
19 risdiction” means any court of the United
20 States organized under Article III of the
21 Constitution of the United States, the
22 court organized under the Foreign Intel-
23 ligence Surveillance Act of 1978 (50 U.S.C.
24 1801 et seq.), or a court of general crimi-
25 nal jurisdiction of a State authorized pur-

1 suant to the laws of such State to enter
2 orders authorizing searches and seizures.

3 **[(5) DATA NETWORK SERVICE PRO-**
4 **VIDER.—**The term “data network service
5 provider” means a person offering any
6 service to the general public that pro-
7 vides the users thereof with the ability to
8 transmit or receive data, including com-
9 munications.

10 **[(6) DECRYPTION.—**The term
11 “decryption” means the retransformation
12 or unscrambling of encrypted data, in-
13 cluding communications, to its readable
14 plaintext version. To “decrypt” data, in-
15 cluding communications, is to perform
16 decryption.

17 **[(7) DECRYPTION INFORMATION.—**The
18 term “decryption information” means in-
19 formation or technology that enables one
20 to readily retransform or unscramble
21 encrypted data from its unreadable and
22 incomprehensible format to its readable
23 plaintext version.

24 **[(8) ELECTRONIC STORAGE.—**The term
25 “electronic storage” has the meaning

1 **given that term in section 2510(17) of title**
2 **18, United States Code.**

3 **[(9) ENCRYPTION.—The term**
4 **“encryption” means the transformation**
5 **or scrambling of data, including commu-**
6 **nications, from plaintext to an**
7 **unreadable or incomprehensible format,**
8 **regardless of the technique utilized for**
9 **such transformation or scrambling and**
10 **irrespective of the medium in which such**
11 **data, including communications, occur or**
12 **can be found, for the purposes of protect-**
13 **ing the content of such data, including**
14 **communications. To “encrypt” data, in-**
15 **cluding communications, is to perform**
16 **encryption.**

17 **[(10) ENCRYPTION PRODUCT.—The**
18 **term “encryption product” means any**
19 **software, technology, or mechanism, that**
20 **can be used to encrypt or decrypt, or has**
21 **the capability of encrypting or**
22 **decrypting any data, including commu-**
23 **nications.**

24 **[(11) FOREIGN AVAILABILITY.—The**
25 **term “foreign availability” has the mean-**

1 ing applied to foreign availability of
2 encryption products subject to controls
3 under the Export Administration Regula-
4 tions, as in effect on September 1, 1997.

5 **[(12) GOVERNMENT.—**The term “Gov-
6 ernment” means the Government of the
7 United States and any agency or instru-
8 mentality thereof, or the government of
9 any State.

10 **[(13) INVESTIGATIVE OR LAW ENFORCE-**
11 **MENT OFFICER.—**The term “investigative
12 or law enforcement officer” has the
13 meaning given that term in section
14 2510(7) of title 18, United States Code.

15 **[(14) KEY RECOVERY AGENT.—**The
16 term “key recovery agent” means a per-
17 son trusted by another person or persons
18 to hold and maintain sufficient
19 decryption information to allow for the
20 immediate decryption of the encrypted
21 data or communications of another per-
22 son or persons for whom that informa-
23 tion is held, and who holds and maintains
24 that information as a business or govern-
25 mental practice, whether or not for prof-

1 it. The term “key recovery agent” in-
2 cludes any person who holds his or her
3 decryption information.

4 **[(15) NATIONAL SECURITY.—**The term
5 “national security” means the national
6 defense, foreign relations, or economic
7 interests of the United States.

8 **[(16) PLAINTEXT.—**The term
9 “plaintext” means the readable or com-
10 prehensible format of data, including
11 communications, prior to its being
12 encrypted or after it has been decrypted.

13 **[(17) PLAINVOICE.—**The term
14 “plainvoice” means communication spe-
15 cific plaintext.

16 **[(18) SECRETARY.—**The term “Sec-
17 retary” means the Secretary of Com-
18 merce, unless otherwise specifically iden-
19 tified.

20 **[(19) STATE.—**The term “State” has
21 the meaning given that term in section
22 2510(3) of title 18, United States Code.

23 **[(20) TELECOMMUNICATIONS CAR-**
24 **RIER.—**The term “telecommunications
25 carrier” has the meaning given that term

1 in section 102(8) of the Communications
2 Assistance for Law Enforcement Act (47
3 U.S.C. 1001(8)).

4 **[(21) TELECOMMUNICATIONS SYSTEM.—**
5 **The term “telecommunications system”**
6 **means any equipment, technology, or re-**
7 **lated software used in the movement,**
8 **switching, interchange, transmission, re-**
9 **ception, or internal signaling of data, in-**
10 **cluding communications over wire, fiber**
11 **optic, radio frequency, or other medium.**

12 **[(22) UNITED STATES PERSON.—The**
13 **term “United States person” means—**

14 **[(A) any citizen of the United**
15 **States;**

16 **[(B) any other person organized**
17 **under the laws of any State; and**

18 **[(C) any person organized under**
19 **the laws of any foreign country who**
20 **is owned or controlled by individuals**
21 **or persons described in subpara-**
22 **graphs (A) and (B).**

23 **[[SEC. 102. LAWFUL USE OF ENCRYPTION.**

24 **[[Except as otherwise provided by this**
25 **Act or otherwise provided by law, it shall be**

1 lawful for any person within any State and for
2 any United States person to use any
3 encryption product, regardless of encryption
4 algorithm selected, encryption key length
5 chosen, or implementation technique or me-
6 dium used.

7 [[SEC. 103. VOLUNTARY PRIVATE SECTOR PARTICIPATION
8 IN KEY MANAGEMENT INFRASTRUCTURE.

9 [[(a) USE IS VOLUNTARY.—The use of cer-
10 tificate authorities or key recovery agents is
11 voluntary.

12 [[(b) REGULATIONS.—The Secretary shall
13 promulgate regulations establishing stand-
14 ards for creating key management infrastruc-
15 tures. Such regulations should—

16 [[(1) allow for the voluntary partici-
17 pation by private persons and non-Fed-
18 eral entities; and

19 [[(2) promote the development of cer-
20 tificate authorities and key recovery
21 agents.

22 [[(c) REGISTRATION OF CERTIFICATE AU-
23 THORITIES AND KEY RECOVERY AGENTS.—Cer-
24 tificate authorities and key recovery agents
25 meeting the standards established by the Sec-

1 retary may be registered by the Secretary if
 2 they so choose, and may identify themselves
 3 as meeting the standards of the Secretary.

4 [[SEC. 104. UNLAWFUL USE OF ENCRYPTION.

5 [[**(a) IN GENERAL.**—Part I of title 18, Unit-
 6 ed States Code, is amended by inserting after
 7 chapter 121 the following new chapter:

8 **“CHAPTER 122—ENCRYPTED DATA, INCLUDING**
 9 **COMMUNICATIONS**

 “Sec.

 [[“2801. Unlawful use of encryption in furtherance of a criminal act.

 [[“2802. Privacy protection.

 [[“2803. Unlawful sale of encryption.

 [[“2804. Encryption products manufactured and intended for use in the United States.

 [[“2805. Injunctive relief and proceedings.

 [[“2806. Court order access to plaintext.

 [[“2807. Notification procedures.

 [[“2808. Lawful use of plaintext or decryption information.

 [[“2809. Identification of decryption information.

 [[“2810. Unlawful export of certain encryption products.

 [[“2811. Definitions.

10 [[“§ 2801. Unlawful use of encryption in furtherance
 11 of a criminal act

12 [[**“(a) PROHIBITED ACTS.**—Whoever know-
 13 ingly uses encryption in furtherance of the
 14 commission of a criminal offense for which
 15 the person may be prosecuted in a district
 16 court of the United States shall—

17 [[**“(1) in the case of a first offense**
 18 under this section, be imprisoned for not

1 more than 5 years, or fined under this
2 title, or both; and

3 [[“(2) in the case of a second or sub-
4 sequent offense under this section, be im-
5 prisoned for not more than 10 years, or
6 fined under this title, or both.

7 [[“(b) CONSECUTIVE SENTENCE.—Notwith-
8 standing any other provision of law, the court
9 shall not place on probation any person con-
10 victed of a violation of this section, nor shall
11 the term of imprisonment imposed under this
12 section run concurrently with any other term
13 of imprisonment imposed for the underlying
14 criminal offense.

15 [[“(c) PROBABLE CAUSE NOT CONSTITUTED
16 BY USE OF ENCRYPTION.—The use of
17 encryption alone shall not constitute prob-
18 able cause to believe that a crime is being or
19 has been committed.

20 [[“§ 2802. Privacy protection

21 [[“(a) IN GENERAL.—It shall be unlawful
22 for any person to intentionally—

23 [[“(1) obtain or use decryption infor-
24 mation without lawful authority for the

1 **purpose of decrypting data, including**
2 **communications;**

3 **[[“(2) exceed lawful authority in**
4 **decrypting data, including communica-**
5 **tions;**

6 **[[“(3) break the encryption code of**
7 **another person without lawful authority**
8 **for the purpose of violating the privacy**
9 **or security of that person or depriving**
10 **that person of any property rights;**

11 **[[“(4) impersonate another person for**
12 **the purpose of obtaining decryption in-**
13 **formation of that person without lawful**
14 **authority;**

15 **[[“(5) facilitate or assist in the**
16 **encryption of data, including communica-**
17 **tions, knowing that such data, including**
18 **communications, are to be used in fur-**
19 **therance of a crime; or**

20 **[[“(6) disclose decryption information**
21 **in violation of a provision of this chapter.**

22 **[[“(b) CRIMINAL PENALTY.—Whoever vio-**
23 **lates this section shall be imprisoned for not**
24 **more than 10 years, or fined under this title,**
25 **or both.**

1 **[[“§ 2803. Unlawful sale of encryption**

2 **[[“Whoever, after January 31, 2000, sells**
3 **in interstate or foreign commerce any**
4 **encryption product that does not include fea-**
5 **tures or functions permitting duly authorized**
6 **persons immediate access to plaintext or im-**
7 **mediate decryption capabilities shall be im-**
8 **prisoned for not more than 5 years, fined**
9 **under this title, or both.**

10 **[[“§ 2804. Encryption products manufactured and in-**
11 **tended for use in the United States**

12 **[[“(a) PUBLIC NETWORK SERVICE PROVID-**
13 **ERS.—After January 31, 2000, public network**
14 **service providers offering encryption prod-**
15 **ucts or encryption services shall ensure that**
16 **such products or services enable the imme-**
17 **diate decryption or access to plaintext of the**
18 **data, including communications, encrypted**
19 **by such products or services on the public**
20 **network upon receipt of a court order or war-**
21 **rant, pursuant to section 2806.**

22 **[[“(b) MANUFACTURERS, DISTRIBUTORS, AND**
23 **IMPORTERS.—After January 31, 2000, it shall be**
24 **unlawful for any person to manufacture for**
25 **distribution, distribute, or import encryption**

1 products intended for sale or use in the Unit-
2 ed States, unless that product—

3 [[“(1) includes features or functions
4 that provide an immediate access to
5 plaintext capability, through any means,
6 mechanism, or technological method
7 that—

8 [[“(A) permits immediate
9 decryption of the encrypted data, in-
10 cluding communications, upon the re-
11 ceipt of decryption information by an
12 authorized party in possession of a
13 facially valid order issued by a court
14 of competent jurisdiction; and

15 [[“(B) allows the decryption of
16 encrypted data, including commu-
17 nications, without the knowledge or
18 cooperation of the person being in-
19 vestigated, subject to the require-
20 ments set forth in section 2806;

21 [[“(2) can be used only on systems or
22 networks that include features or func-
23 tions that provide an immediate access to
24 plaintext capability, through any means,

1 mechanism, or technological method
2 that—

3 [[“(A) permits immediate
4 decryption of the encrypted data, in-
5 cluding communications, upon the re-
6 ceipt of decryption information by an
7 authorized party in possession of a
8 facially valid order issued by a court
9 of competent jurisdiction; and

10 [[“(B) allows the decryption of
11 encrypted data, including commu-
12 nications, without the knowledge or
13 cooperation of the person being in-
14 vestigated, subject to the require-
15 ments set forth in section 2806; or

16 [[“(3) otherwise meets the technical
17 requirements and functional criteria pro-
18 mulgated by the Attorney General under
19 subsection (c).

20 [[“(c) ATTORNEY GENERAL CRITERIA.—

21 [[“(1) PUBLICATION OF REQUIRE-
22 MENTS.—Within 180 days after the date of
23 the enactment of this chapter, the Attor-
24 ney General shall publish in the Federal
25 Register technical requirements and

1 functional criteria for complying with the
2 decryption requirements set forth in this
3 section.

4 **[[“(2) PROCEDURES FOR ADVISORY OPIN-**
5 **IONS.—Within 180 days after the date of**
6 **the enactment of this chapter, the Attor-**
7 **ney General shall promulgate procedures**
8 **by which data network service providers**
9 **and encryption product manufacturers,**
10 **sellers, re-sellers, distributors, and im-**
11 **porters may obtain advisory opinions as**
12 **to whether an encryption product in-**
13 **tended for sale or use in the United**
14 **States after January 31, 2000, meets the**
15 **requirements of this section and the tech-**
16 **nical requirements and functional cri-**
17 **teria promulgated pursuant to paragraph**
18 **(1).**

19 **[[“(3) PARTICULAR METHODOLOGY NOT**
20 **REQUIRED.—Nothing in this chapter or**
21 **any other provision of law shall be con-**
22 **strued as requiring the implementation**
23 **of any particular decryption methodology**
24 **in order to satisfy the requirements of**
25 **subsections (a) and (b), or the technical**

1 requirements and functional criteria re-
2 quired by the Attorney General under
3 paragraph (1).

4 [[“(d) USE OF PRIOR PRODUCTS LAWFUL.—
5 After January 31, 2000, it shall not be unlaw-
6 ful to use any encryption product purchased
7 or in use prior to such date.

8 [[“§ 2805. Injunctive relief and proceedings

9 [[“(a) INJUNCTION.—Whenever it appears
10 to the Secretary or the Attorney General that
11 any person is engaged in, or is about to en-
12 gage in, any act that constitutes, or would
13 constitute, a violation of section 2804, the At-
14 torney General may initiate a civil action in
15 a district court of the United States to enjoin
16 such violation. Upon the filing of the com-
17 plaint seeking injunctive relief by the Attor-
18 ney General, the court shall automatically
19 issue a temporary restraining order against
20 the party being sued.

21 [[“(b) BURDEN OF PROOF.—In a suit
22 brought by the Attorney General under sub-
23 section (a), the burden shall be upon the Gov-
24 ernment to establish by a preponderance of
25 the evidence that the encryption product in-

1 involved does not comport with the require-
2 ments set forth by the Attorney General pur-
3 suant to section 2804 providing for immediate
4 access to plaintext by Federal, State, or local
5 authorities.

6 [[“(c) CLOSING OF PROCEEDINGS.—(1) Upon
7 motion of the party against whom injunction
8 is being sought—

9 [[“(A) any or all of the proceedings
10 under this section shall be closed to the
11 public; and

12 [[“(B) public disclosure of the pro-
13 ceedings shall be treated as contempt of
14 court.

15 [[“(2) Upon a written finding by the court
16 that public disclosure of information relevant
17 to the prosecution of the injunction or rel-
18 evant to a determination of the factual or
19 legal issues raised in the case would cause ir-
20 reparable or financial harm to the party
21 against whom the suit is brought, or would
22 otherwise disclose proprietary information of
23 any party to the case, all proceedings shall be
24 closed to members of the public, except the
25 parties to the suit, and all transcripts, mo-

1 tions, and orders shall be placed under seal to
2 protect their disclosure to the general public.

3 [[“(d) ADVISORY OPINION AS DEFENSE.—It
4 is an absolute defense to a suit under this sub-
5 section that the party against whom suit is
6 brought obtained an advisory opinion from
7 the Attorney General pursuant to section
8 2804(c) and that the product at issue in the
9 suit comports in every aspect with the re-
10 quirements announced in such advisory opin-
11 ion.

12 [[“(e) BASIS FOR PERMANENT INJUNCTION.—
13 The court shall issue a permanent injunction
14 against the distribution of, and any future
15 manufacture of, the encryption product at
16 issue in the suit filed under subsection (a) if
17 the court finds by a preponderance of the evi-
18 dence that the product does not meet the re-
19 quirements set forth by the Attorney General
20 pursuant to section 2804 providing for imme-
21 diate access to plaintext by Federal, State, or
22 local authorities.

23 [[“(f) APPEALS.—Either party may appeal,
24 to the appellate court with jurisdiction of the
25 case, any adverse ruling by the district court

1 entered pursuant to this section. For the pur-
2 poses of appeal, the parties shall be governed
3 by the Federal Rules of Appellate Procedure,
4 except that the Government shall file its no-
5 tice of appeal not later than 30 days after the
6 entry of the final order on the docket of the
7 district court. The appeal of such matter shall
8 be considered on an expedited basis and re-
9 solved as soon as practicable.

10 [[“§ 2806. Court order access to plaintext

11 [[“(a) COURT ORDER.—(1) A court of com-
12 petent jurisdiction shall issue an order, ex
13 parte, granting an investigative or law en-
14 forcement officer immediate access to the
15 plaintext of encrypted data, including com-
16 munications, or requiring any person in pos-
17 session of decryption information to provide
18 such information to a duly authorized inves-
19 tigative or law enforcement officer—

20 [[“(A) upon the application by an at-
21 torney for the Government that—

22 [[“(i) is made under oath or affir-
23 mation by the attorney for the Gov-
24 ernment; and

1 **[[“(ii) provides a factual basis es-**
2 **tablishing the relevance that the**
3 **plaintext or decryption information**
4 **being sought has to a law enforce-**
5 **ment or foreign counterintelligence**
6 **investigation then being conducted**
7 **pursuant to lawful authorities; and**

8 **[[“(B) if the court finds, in writing,**
9 **that the plaintext or decryption informa-**
10 **tion being sought is relevant to an ongoing**
11 **lawful law enforcement or foreign**
12 **counterintelligence investigation and the**
13 **investigative or law enforcement officer**
14 **is entitled to such plaintext or decryption**
15 **information.**

16 **[[“(2) The order issued by the court under**
17 **this section shall be placed under seal, except**
18 **that a copy may be made available to the in-**
19 **vestigative or law enforcement officer author-**
20 **ized to obtain access to the plaintext of the**
21 **encrypted information, or authorized to ob-**
22 **tain the decryption information sought in the**
23 **application. Such order shall also be made**
24 **available to the person responsible for provid-**
25 **ing the plaintext or the decryption informa-**

1 tion, pursuant to such order, to the investiga-
2 tive or law enforcement officer.

3 [[“(3) Disclosure of an application made,
4 or order issued, under this section, is not au-
5 thorized, except as may otherwise be specifi-
6 cally permitted by this section or another
7 order of the court.

8 [[“(b) OTHER ORDERS.—An attorney for
9 the Government may make application to a
10 district court of the United States for an order
11 under subsection (a), upon a request from a
12 foreign country pursuant to a Mutual Legal
13 Assistance Treaty with such country that is in
14 effect at the time of the request from such
15 country.

16 [[“(c) RECORD OF ACCESS REQUIRED.—(1)
17 There shall be created an electronic record,
18 or similar type record, of each instance in
19 which an investigative or law enforcement of-
20 ficer, pursuant to an order under this section,
21 gains access to the plaintext of otherwise
22 encrypted information, or is provided
23 decryption information, without the knowl-
24 edge or consent of the owner of the data, in-

1 cluding communications, who is the user of
2 the encryption product involved.

3 [[“(2) The court issuing the order under
4 this section shall require that the electronic
5 or similar type of record described in para-
6 graph (1) is maintained in a place and a man-
7 ner that is not within the custody or control
8 of an investigative or law enforcement officer
9 gaining the access or provided the decryption
10 information. The record shall be tendered to
11 the court, upon notice from the court.

12 [[“(3) The court receiving such electronic
13 or similar type of record described in para-
14 graph (1) shall make the original and a cer-
15 tified copy of the record available to the attor-
16 ney for the Government making application
17 under this section, and to the attorney for, or
18 directly to, the owner of the data, including
19 communications, who is the user of the
20 encryption product.

21 [[“(d) AUTHORITY TO INTERCEPT COMMU-
22 NICATIONS NOT INCREASED.—Nothing in this
23 chapter shall be construed to enlarge or mod-
24 ify the circumstances or procedures under
25 which a Government entity is entitled to

1 intercept or obtain oral, wire, or electronic
2 communications or information.

3 [[“(e) CONSTRUCTION.—This chapter shall
4 be strictly construed to apply only to a Gov-
5 ernment entity’s ability to decrypt data, in-
6 cluding communications, for which it has pre-
7 viously obtained lawful authority to intercept
8 or obtain pursuant to other lawful authorities
9 that would otherwise remain encrypted.

10 [[“§ 2807. Notification procedures

11 [[“(a) IN GENERAL.—Within a reasonable
12 time, but not later than 90 days after the filing
13 of an application for an order under section
14 2806 which is granted, the court shall cause
15 to be served, on the persons named in the
16 order or the application, and such other par-
17 ties whose decryption information or whose
18 plaintext has been provided to an investiga-
19 tive or law enforcement officer pursuant to
20 this chapter as the court may determine that
21 is in the interest of justice, an inventory
22 which shall include notice of—

23 [[“(1) the fact of the entry of the
24 order or the application;

1 **[[“(2) the date of the entry of the ap-**
2 **plication and issuance of the order; and**

3 **[[“(3) the fact that the person’s**
4 **decryption information or plaintext data,**
5 **including communications, have been**
6 **provided or accessed by an investigative**
7 **or law enforcement officer.**

8 **The court, upon the filing of a motion, may**
9 **make available to that person or that person’s**
10 **counsel, for inspection, such portions of the**
11 **plaintext, applications, and orders as the**
12 **court determines to be in the interest of jus-**
13 **tice. On an ex parte showing of good cause to**
14 **a court of competent jurisdiction, the serving**
15 **of the inventory required by this subsection**
16 **may be postponed.**

17 **[[“(b) ADMISSION INTO EVIDENCE.—The**
18 **contents of any encrypted information that**
19 **has been obtained pursuant to this chapter or**
20 **evidence derived therefrom shall not be re-**
21 **ceived in evidence or otherwise disclosed in**
22 **any trial, hearing, or other proceeding in a**
23 **Federal or State court unless each party, not**
24 **less than 10 days before the trial, hearing, or**
25 **proceeding, has been furnished with a copy of**

1 the order, and accompanying application,
2 under which the decryption or access to
3 plaintext was authorized or approved. This
4 10-day period may be waived by the court if
5 the court finds that it was not possible to fur-
6 nish the party with the information described
7 in the preceding sentence within 10 days be-
8 fore the trial, hearing, or proceeding and that
9 the party will not be prejudiced by the delay
10 in receiving such information.

11 [[“(c) CONTEMPT.—Any violation of the
12 provisions of this section may be punished by
13 the court as a contempt thereof.

14 [[“(d) MOTION TO SUPPRESS.—Any ag-
15 grieved person in any trial, hearing, or pro-
16 ceeding in or before any court, department,
17 officer, agency, regulatory body, or other au-
18 thority of the United States or a State may
19 move to suppress the contents of any
20 decrypted data, including communications,
21 obtained pursuant to this chapter, or evi-
22 dence derived therefrom, on the grounds
23 that —

24 [[“(1) the plaintext was unlawfully
25 decrypted or accessed;

1 **[[“(2) the order of authorization or**
2 **approval under which it was decrypted**
3 **or accessed is insufficient on its face; or**

4 **[[“(3) the decryption was not made in**
5 **conformity with the order of authoriza-**
6 **tion or approval.**

7 **Such motion shall be made before the trial,**
8 **hearing, or proceeding unless there was no**
9 **opportunity to make such motion, or the per-**
10 **son was not aware of the grounds of the mo-**
11 **tion. If the motion is granted, the plaintext of**
12 **the decrypted data, including communica-**
13 **tions, or evidence derived therefrom, shall be**
14 **treated as having been obtained in violation**
15 **of this chapter. The court, upon the filing of**
16 **such motion by the aggrieved person, may**
17 **make available to the aggrieved person or**
18 **that person’s counsel for inspection such por-**
19 **tions of the decrypted plaintext, or evidence**
20 **derived therefrom, as the court determines to**
21 **be in the interests of justice.**

22 **[[“(e) APPEAL BY UNITED STATES.—In addi-**
23 **tion to any other right to appeal, the United**
24 **States shall have the right to appeal from an**
25 **order granting a motion to suppress made**

1 under subsection (d), or the denial of an appli-
2 cation for an order under section 2806, if the
3 United States attorney certifies to the court
4 or other official granting such motion or de-
5 nying such application that the appeal is not
6 taken for purposes of delay. Such appeal shall
7 be taken within 30 days after the date the
8 order was entered on the docket and shall be
9 diligently prosecuted.

10 [[“(f) CIVIL ACTION FOR VIOLATION.—Ex-
11 cept as otherwise provided in this chapter,
12 any person described in subsection (g) may in
13 a civil action recover from the United States
14 Government the actual damages suffered by
15 the person as a result of a violation described
16 in that subsection, reasonable attorney’s fees,
17 and other litigation costs reasonably incurred
18 in prosecuting such claim.

19 [[“(g) COVERED PERSONS.—Subsection (f)
20 applies to any person whose decryption infor-
21 mation—

22 [[“(1) is knowingly obtained without
23 lawful authority by an investigative or
24 law enforcement officer;

1 **[[“(2) is obtained by an investigative**
2 **or law enforcement officer with lawful**
3 **authority and is knowingly used or dis-**
4 **closed by such officer unlawfully; or**

5 **[[“(3) is obtained by an investigative**
6 **or law enforcement officer with lawful**
7 **authority and whose decryption informa-**
8 **tion is unlawfully used to disclose the**
9 **plaintext of the data, including commu-**
10 **nications.**

11 **[[“(h) LIMITATION.—A civil action under**
12 **subsection (f) shall be commenced not later**
13 **than 2 years after the date on which the un-**
14 **lawful action took place, or 2 years after the**
15 **date on which the claimant first discovers the**
16 **violation, whichever is later.**

17 **[[“(i) EXCLUSIVE REMEDIES.—The remedies**
18 **and sanctions described in this chapter with**
19 **respect to the decryption of data, including**
20 **communications, are the only judicial rem-**
21 **edies and sanctions for violations of this**
22 **chapter involving such decryptions, other**
23 **than violations based on the deprivation of**
24 **any rights, privileges, or immunities secured**
25 **by the Constitution.**

1 **[(“j) TECHNICAL ASSISTANCE BY PROVID-**
2 **ERS.—A provider of encryption technology or**
3 **network service that has received an order is-**
4 **sued by a court pursuant to this chapter shall**
5 **provide to the investigative or law enforce-**
6 **ment officer concerned such technical assist-**
7 **ance as is necessary to execute the order.**
8 **Such provider may, however, move the court**
9 **to modify or quash the order on the ground**
10 **that its assistance with respect to the**
11 **decryption or access to plaintext cannot be**
12 **performed in a timely or reasonable fashion.**
13 **The court, upon notice to the Government,**
14 **shall decide such motion expeditiously.**

15 **[(“k) REPORTS TO CONGRESS.—In May of**
16 **each year, the Attorney General, or an Assist-**
17 **ant Attorney General specifically designated**
18 **by the Attorney General, shall report in writ-**
19 **ing to Congress on the number of applications**
20 **made and orders entered authorizing Federal,**
21 **State, and local law enforcement access to**
22 **decryption information for the purposes of**
23 **reading the plaintext of otherwise encrypted**
24 **data, including communications, pursuant to**
25 **this chapter. Such reports shall be submitted**

1 to the Committees on the Judiciary of the
2 House of Representatives and of the Senate,
3 and to the Permanent Select Committee on In-
4 telligence for the House of Representatives
5 and the Select Committee on Intelligence for
6 the Senate.

7 [[“§ 2808. Lawful use of plaintext or decryption infor-
8 mation

9 [[“(a) AUTHORIZED USE OF DECRYPTION IN-
10 FORMATION.—

11 [[“(1) CRIMINAL INVESTIGATIONS.—An
12 investigative or law enforcement officer
13 to whom plaintext or decryption informa-
14 tion is provided may use such plaintext
15 or decryption information for the pur-
16 poses of conducting a lawful criminal in-
17 vestigation or foreign counterintelligence
18 investigation, and for the purposes of
19 preparing for and prosecuting any crimi-
20 nal violation of law.

21 [[“(2) CIVIL REDRESS.—Any plaintext
22 or decryption information provided
23 under this chapter to an investigative or
24 law enforcement officer may not be dis-
25 closed, except by court order, to any

1 other person for use in a civil proceeding
2 that is unrelated to a criminal investiga-
3 tion and prosecution for which the
4 plaintext or decryption information is au-
5 thorized under paragraph (1). Such order
6 shall only issue upon a showing by the
7 party seeking disclosure that there is no
8 alternative means of obtaining the
9 plaintext, or decryption information,
10 being sought and the court also finds that
11 the interests of justice would not be
12 served by nondisclosure.

13 [[“(b) LIMITATION.—An investigative or
14 law enforcement officer may not use
15 decryption information obtained under this
16 chapter to determine the plaintext of any
17 data, including communications, unless it has
18 obtained lawful authority to obtain such data,
19 including communications, under other law-
20 ful authorities.

21 [[“(c) RETURN OF DECRYPTION INFORMA-
22 TION.—An attorney for the Government shall,
23 upon the issuance of an order of a court of
24 competent jurisdiction—

1 **[[“(1)(A) return any decryption infor-**
2 **mation to the person responsible for pro-**
3 **viding it to an investigative or law en-**
4 **forcement officer pursuant to this chap-**
5 **ter; or**

6 **[[“(B) destroy such decryption infor-**
7 **mation, if the court finds that the inter-**
8 **ests of justice or public safety require**
9 **that such decryption information should**
10 **not be returned to the provider; and**

11 **[[“(2) within 10 days after execution**
12 **of the court’s order to destroy the**
13 **decryption information—**

14 **[[“(A) certify to the court that the**
15 **decryption information has either**
16 **been returned or destroyed consist-**
17 **ent with the court’s order; and**

18 **[[“(B) notify the provider of the**
19 **decryption information of the de-**
20 **struction of such information.**

21 **[[“(d) OTHER DISCLOSURE OF DECRYPTION**
22 **INFORMATION.—Except as otherwise provided**
23 **in section 2806, a key recovery agent may not**
24 **disclose decryption information stored with**

1 the key recovery agent by a person unless the
2 disclosure is—

3 [[“(1) to the person, or an authorized
4 agent thereof;

5 [[“(2) with the consent of the person,
6 including pursuant to a contract entered
7 into with the person;

8 [[“(3) pursuant to a court order upon
9 a showing of compelling need for the in-
10 formation that cannot be accommodated
11 by any other means if—

12 [[“(A) the person who supplied
13 the information is given reasonable
14 notice, by the person seeking the dis-
15 closure, of the court proceeding rel-
16 evant to the issuance of the court
17 order; and

18 [[“(B) the person who supplied
19 the information is afforded the oppor-
20 tunity to appear in the court proceed-
21 ing and contest the claim of the per-
22 son seeking the disclosure;

23 [[“(4) pursuant to a determination by
24 a court of competent jurisdiction that an-
25 other person is lawfully entitled to hold

1 such decryption information, including
2 determinations arising from legal pro-
3 ceedings associated with the incapacity,
4 death, or dissolution of any person; or

5 [[“(5) otherwise permitted by a provi-
6 sion of this chapter or otherwise per-
7 mitted by law.

8 [[“§ 2809. Identification of decryption information

9 [[“(a) IDENTIFICATION.—To avoid inadvert-
10 ent disclosure, any person who provides
11 decryption information to an investigative or
12 law enforcement officer pursuant to this
13 chapter shall specifically identify that part of
14 the material provided that discloses
15 decryption information as such.

16 [[“(b) RESPONSIBILITY OF INVESTIGATIVE OR
17 LAW ENFORCEMENT OFFICER.—The investiga-
18 tive or law enforcement officer receiving any
19 decryption information under this chapter
20 shall maintain such information in facilities
21 and in a method so as to reasonably assure
22 that inadvertent disclosure does not occur.

1 **[[“§ 2810. Unlawful export of certain encryption**
2 **products**

3 **[[“Whoever, after January 31, 2000, know-**
4 **ingly exports an encryption product that does**
5 **not include features or functions providing**
6 **duly authorized persons immediate access to**
7 **plaintext or immediate decryption capabili-**
8 **ties, as required under law, shall be impris-**
9 **oned for not more than 5 years, fined under**
10 **this title, or both.**

11 **[[“§ 2811. Definitions**

12 **[[“The definitions set forth in section 101**
13 **of the Security and Freedom through**
14 **Encryption (‘SAFE’) Act of 1997 shall apply to**
15 **this chapter.”.**

16 **[[(b) CONFORMING AMENDMENT.—The table**
17 **of chapters for part I of title 18, United States**
18 **Code, is amended by inserting after the item**
19 **relating to chapter 121 the following new**
20 **item:**

[[“122. Encrypted data, including communications 2801”.

1 **[[TITLE II—GOVERNMENT**
2 **PROCUREMENT**

3 **[[SEC. 201. FEDERAL PURCHASES OF ENCRYPTION PROD-**
4 **UCTS.**

5 **[[After January 1, 1999, any encryption**
6 **product or service purchased or otherwise**
7 **procured by the United States Government to**
8 **provide the security service of data confiden-**
9 **tiality for a Federal computer system shall in-**
10 **clude a technique enabling immediate**
11 **decryption by an authorized party without**
12 **the knowledge or cooperation of the person**
13 **using such encryption products or services.**

14 **[[SEC. 202. ENCRYPTION PRODUCTS PURCHASED WITH**
15 **FEDERAL FUNDS.**

16 **[[After January 1, 1999, any encryption**
17 **product or service purchased directly with**
18 **Federal funds to provide the security service**
19 **of data confidentiality shall include a tech-**
20 **nique enabling immediate decryption by an**
21 **authorized party without the knowledge or**
22 **cooperation of the person using such**
23 **encryption product or service unless the Sec-**
24 **retary, with the concurrence of the Attorney**
25 **General, determines implementing this re-**

1 requirement would not promote the purposes of
2 this Act.

3 [[SEC. 203. NETWORKS ESTABLISHED WITH FEDERAL
4 FUNDS.

5 [[After January 1, 1999, any communica-
6 tions network established with the use of Fed-
7 eral funds shall use encryption products
8 which include techniques enabling immediate
9 decryption by an authorized party without
10 the knowledge or cooperation of the person
11 using such encryption products or services
12 unless the Secretary, with the concurrence of
13 the Attorney General, determines implement-
14 ing this requirement would not promote the
15 purposes of this Act.

16 [[SEC. 204. PRODUCT LABELS.

17 [[An encryption product may be labeled
18 to inform users that the product is authorized
19 for sale to or for use in transactions and com-
20 munications with the United States Govern-
21 ment under this title.

22 [[SEC. 205. NO PRIVATE MANDATE.

23 [[The United States Government may not
24 mandate the use of encryption standards for
25 the private sector other than for use with

1 computer systems, networks, or other systems
2 of the United States Government, or systems
3 or networks created using Federal funds.

4 [[SEC. 206. IMPLEMENTATION.

5 **[[(a) EXCLUSION.—**Nothing in this title
6 shall apply to encryption products and serv-
7 ices used solely for access control, authentica-
8 tion, integrity, nonrepudiation, digital signa-
9 tures, or other similar purposes.

10 **[[(b) RULEMAKING.—**The Secretary, in con-
11 sultation with the Attorney General and other
12 affected agencies, may through rules provide
13 for the orderly implementation of this title
14 and the effective use of secure public net-
15 works.

16 **[[TITLE III—EXPORTS OF**
17 **ENCRYPTION**

18 [[SEC. 301. EXPORTS OF ENCRYPTION.

19 **[[(a) COORDINATION OF EXECUTIVE BRANCH**
20 **AGENCIES REQUIRED.—**The Secretary, in close
21 coordination with the Secretary of Defense
22 and any other executive branch department
23 or agency with responsibility for protecting
24 the national security, shall have the authority
25 to control the export of encryption products

1 **not controlled on the United States Munitions**
2 **List.**

3 **[(b) DECISIONS NOT SUBJECT TO JUDICIAL**
4 **REVIEW.—Decisions made by the Secretary**
5 **pursuant to subsection (a) with respect to ex-**
6 **ports of encryption products under this title**
7 **shall not be subject to judicial review.**

8 **[[SEC. 302. LICENSE EXCEPTION FOR CERTAIN**
9 **ENCRYPTION PRODUCTS.**

10 **[(a) LICENSE EXCEPTION.—After January**
11 **31, 2000, encryption products, without regard**
12 **to encryption strength, shall be eligible for ex-**
13 **port under a license exception if such**
14 **encryption product—**

15 **[(1) is submitted to the Secretary for**
16 **a 1-time product review;**

17 **[(2) does not include features or**
18 **functions that would otherwise require li-**
19 **censing under applicable regulations;**

20 **[(3) is not destined for countries,**
21 **end users, or end uses that the Secretary,**
22 **in coordination with the Secretary of De-**
23 **fense and other executive branch depart-**
24 **ments or agencies with responsibility for**
25 **protecting the national security, by regu-**

1 lation, has determined should be ineli-
2 gible to receive such products, and is oth-
3 erwise qualified for export; and

4 [[(4)(A) includes features or func-
5 tions providing an immediate access to
6 plaintext capability, if there is lawful au-
7 thority for such immediate access; or

8 [[(B) includes features or functions
9 providing an immediate decryption capa-
10 bility of the encrypted data, including
11 communications, upon the receipt of
12 decryption information by an authorized
13 party, and such decryption can be accom-
14 plished without unauthorized disclosure.

15 [[(b) ENABLING OF DECRYPTION CAPABILI-
16 TIES.—The features or functions described in
17 subsection (a)(4) need not be enabled by the
18 manufacturer before or at the time of export
19 for purposes of this title. Such features or
20 functions may be enabled by the purchaser or
21 end user.

22 [[(c) RESPONSIBILITIES OF THE SEC-
23 RETARY.—The Secretary, in close coordination
24 with the Secretary of Defense and other exec-
25 utive branch departments or agencies with

1 responsibility for protecting the national se-
2 curity, shall—

3 **[(1) specify, by regulation, the infor-**
4 **mation that must be submitted for the 1-**
5 **time review referred to in this section;**
6 **and**

7 **[(2) make all export determinations**
8 **under this title within 30 days following**
9 **the date of submission to the Secretary**
10 **of—**

11 **[(A) the completed application**
12 **for a license exception; and**

13 **[(B) the encryption product in-**
14 **tended for export that is to be re-**
15 **viewed as required by this section.**

16 **[(d) EXERCISE OF OTHER AUTHORITIES.—**
17 **The Secretary, and the Secretary of Defense,**
18 **may exercise the authorities they have under**
19 **other provisions of law, including the Export**
20 **Administration Act of 1979, as continued in ef-**
21 **fect under the International Emergency Eco-**
22 **nomic Powers Act, to carry out this section.**

23 **[(e) PRESUMPTION IN FAVOR OF EXPORTS.—**
24 **There shall be a presumption in favor of ex-**
25 **port of encryption products under this title.**

1 **[(f) WAIVER AUTHORITY.—The President**
2 **may by Executive order waive any provision**
3 **of this title, or the applicability of any such**
4 **provision to a person or entity, if the Presi-**
5 **dent determines that the waiver is in the in-**
6 **terests of national security or public safety**
7 **and security. The President shall submit a re-**
8 **port to the relevant committees of the Con-**
9 **gress not later than 15 days after such deter-**
10 **mination. The report shall include the factual**
11 **basis upon which such determination was**
12 **made. The report may be in classified format.**

13 **[(g) RELEVANT COMMITTEES.—The rel-**
14 **evant committees of the Congress described**
15 **in subsection (f) are the Committee on Inter-**
16 **national Relations, the Committee on the Ju-**
17 **diciary, the Committee on National Security,**
18 **and the Permanent Select Committee on In-**
19 **telligence of the House of Representatives,**
20 **and the Committee on Foreign Relations, the**
21 **Committee on the Judiciary, the Committee**
22 **on Armed Services, and the Select Committee**
23 **on Intelligence of the Senate.**

1 **[[SEC. 303. LICENSE EXCEPTION FOR TELECOMMUNI-**
2 **CATIONS PRODUCTS.**

3 **[[After a 1-time review as described in**
4 **section 302, the Secretary shall authorize for**
5 **export under a license exception voice**
6 **encryption products that do not contain**
7 **decryption or access to plainvoice features or**
8 **functions otherwise required in section 302, if**
9 **the Secretary, after consultation with rel-**
10 **evant executive branch departments or agen-**
11 **cies, determines that—**

12 **[[**(1) **information recovery require-**
13 **ments for such exports would disadvan-**
14 **tage United States exporters; and**

15 **[[**(2) **such exports under a license ex-**
16 **ception would not create a risk to the for-**
17 **foreign policy, non-proliferation, or national**
18 **security of the United States.**

19 **[[SEC. 304. REVIEW FOR CERTAIN INSTITUTIONS.**

20 **[[The Secretary, in consultation with**
21 **other executive branch departments or agen-**
22 **cies, shall establish a procedure for expedited**
23 **review of export license applications involv-**
24 **ing encryption products for use by qualified**
25 **banks, financial institutions, subsidiaries of**
26 **companies owned or controlled by United**

1 States persons, or other users specifically au-
2 thorized by the Secretary.

3 [[SEC. 305. ENCRYPTION INDUSTRY AND INFORMATION SE-
4 CURITY BOARD.

5 [[(a) ENCRYPTION INDUSTRY AND INFORMA-
6 TION SECURITY BOARD ESTABLISHED.—There is
7 hereby established an Encryption Industry
8 and Information Security Board. The Board
9 shall undertake an advisory role for the Presi-
10 dent.

11 [[(b) PURPOSES.—The purposes of the
12 Board are—

13 [[(1) to provide a forum to foster
14 communication and coordination be-
15 tween industry and the Federal Govern-
16 ment on matters relating to the use of
17 encryption products;

18 [[(2) to promote the export of
19 encryption products manufactured in the
20 United States;

21 [[(3) to encourage research and de-
22 velopment of products that will foster
23 electronic commerce;

24 [[(4) to recommend policies enhanc-
25 ing the security of public networks;

1 **[(5) to promote the protection of in-**
2 **tellectual property and privacy rights of**
3 **individuals using public networks;**

4 **[(6) to enable the United States to**
5 **effectively and continually understand**
6 **the benefits and risks to its national se-**
7 **curity, law enforcement, and public safe-**
8 **ty interests by virtue of the proliferation**
9 **of strong encryption on the global mar-**
10 **ket;**

11 **[(7) to evaluate and make rec-**
12 **ommendations regarding the further de-**
13 **velopment and use of encryption;**

14 **[(8) to advance the development of**
15 **international standards regarding inter-**
16 **operability and global use of encryption**
17 **products; and**

18 **[(9) to evaluate the foreign availabil-**
19 **ity of encryption products and their**
20 **threat to United States industry.**

21 **[(c) MEMBERSHIP.—(1) The Board shall be**
22 **composed of 13 members, as follows:**

23 **[(A) The Secretary, or the Sec-**
24 **retary's designee, who shall chair the**
25 **Board.**

1 **[(B) The Attorney General, or the**
2 **Director of the Federal Bureau of Inves-**
3 **tigation, or a respective designee.**

4 **[(C) The Secretary of Defense, or the**
5 **Secretary's designee.**

6 **[(D) the Director of Central Intel-**
7 **ligence, or his or her designee.**

8 **[(E) The Special Assistant to the**
9 **President for National Security Affairs,**
10 **or his or her designee.**

11 **[(F) Two private sector individuals,**
12 **appointed by the President, who have ex-**
13 **pertise in consumer and privacy interests**
14 **relating to or affected by information se-**
15 **curity technology.**

16 **[(G) Six representatives from the**
17 **private sector who have expertise in the**
18 **development, operation, marketing, law,**
19 **or public policy relating to information**
20 **security or technology.**

21 **[(2) The six private sector representa-**
22 **tives described in paragraph (1)(G) shall be**
23 **appointed as follows:**

24 **[(A) Two by the Speaker of the**
25 **House of Representatives.**

1 **[(B) One by the Minority Leader**
2 **of the House of Representatives.**

3 **[(C) Two by the Majority Leader**
4 **of the Senate.**

5 **[(D) One by the Minority Leader**
6 **of the Senate.**

7 **[(e) MEETINGS.—The Board shall meet at**
8 **such times and in such places as the Sec-**
9 **retary may prescribe, but not less frequently**
10 **than every four months. The Federal Advisory**
11 **Committee Act (5 U.S.C. App.) does not apply**
12 **to the Board or to meetings held by the Board**
13 **under this section.**

14 **[(f) FINDINGS AND RECOMMENDATIONS.—**
15 **The chair of the Board shall convey the find-**
16 **ings and recommendations of the Board to the**
17 **President and to the Congress within 30 days**
18 **after each meeting of the Board. The rec-**
19 **ommendations of the Board are not binding**
20 **upon the President.**

21 **[(g) FOREIGN AVAILABILITY.—The consid-**
22 **eration of foreign availability by the Board**
23 **shall include computer software that is dis-**
24 **tributed over the Internet or advertised for**
25 **sale, license, or transfer, including over-the-**

1 counter retail sales, mail order transactions,
2 telephone order transactions, electronic dis-
3 tribution, or sale on approval.

4 **[[TITLE IV—LIABILITY** 5 **LIMITATIONS**

6 **[[SEC. 401. COMPLIANCE WITH COURT ORDER.**

7 **[[(a) NO LIABILITY FOR COMPLIANCE.—Sub-**
8 **ject to subsection (b), no civil or criminal li-**
9 **ability under this Act, or under any other pro-**
10 **vision of law, shall attach to any person for**
11 **disclosing or providing—**

12 **[[(1) the plaintext of encrypted data,**
13 **including communications;**

14 **[[(2) the decryption information of**
15 **such encrypted data, including commu-**
16 **nications; or**

17 **[[(3) technical assistance for access**
18 **to the plaintext of, or decryption informa-**
19 **tion for, encrypted data, including com-**
20 **munications.**

21 **[[(b) EXCEPTION.—Subsection (a) shall not**
22 **apply to a person who provides plaintext or**
23 **decryption information to another and is not**
24 **authorized by court order to disclose such**
25 **plaintext or decryption information.**

1 **[[SEC. 402. COMPLIANCE DEFENSE.**

2 **[[Compliance with the provisions of sec-**
3 **tions 2806, 2807, 2808, or 2809 of title 18, Unit-**
4 **ed States Code, as added by section 104(a) of**
5 **this Act, or any regulations authorized there-**
6 **under, shall provide a complete defense for**
7 **any civil action for damages based upon ac-**
8 **tivities covered by this Act, other than an ac-**
9 **tion founded on contract.**

10 **[[SEC. 403. REASONABLE CARE DEFENSE.**

11 **[[The participation by person in the key**
12 **management infrastructure established by**
13 **regulation for United States Government in-**
14 **formation security operations under section**
15 **103 shall be treated as evidence of reasonable**
16 **care or due diligence in any proceeding**
17 **where the reasonableness of one's actions is**
18 **an element of the claim at issue.**

19 **[[SEC. 404. GOOD FAITH DEFENSE.**

20 **[[An objectively reasonable reliance on**
21 **the legal authority provided by this Act and**
22 **the amendments made by this Act, requiring**
23 **or authorizing access to the plaintext of oth-**
24 **erwise encrypted data, including communica-**
25 **tions, or to the decryption information that**
26 **will allow the immediate decryption of data,**

1 including communications, that is otherwise
2 encrypted, shall be a complete defense to any
3 criminal or civil action that may be brought
4 under the laws of the United States or any
5 State.

6 [[SEC. 405. SOVEREIGN IMMUNITY.

7 [[Except as otherwise specifically pro-
8 vided otherwise, nothing in this Act or the
9 amendments made by this Act, or any regula-
10 tions promulgated thereunder, modifies or
11 amends the sovereign immunity of the United
12 States.

13 [[SEC. 406. CIVIL ACTION, GENERALLY.

14 [[A civil action may be brought against
15 any person who, regardless of that person's
16 participation in the key management infra-
17 structure to be established by regulations
18 promulgated by the Secretary pursuant to
19 section 103, violates or acts in a manner that
20 is inconsistent with or violates the provisions
21 or intent of this Act or the amendments made
22 by this Act.

1 **[[TITLE V—INTERNATIONAL**
2 **AGREEMENTS**

3 **[[SEC. 501. SENSE OF CONGRESS.**

4 **[[It is the sense of Congress that—**

5 **[[(1) the President should conduct**
6 **negotiations with foreign governments**
7 **for the purposes of mutual recognition of**
8 **any key management infrastructures, and**
9 **their component parts, that exist or are**
10 **developed; and**

11 **[[(2) such mutual recognition agree-**
12 **ments will safeguard the privacy of the**
13 **citizens of the United States, prevent eco-**
14 **nomic espionage, and enhance the infor-**
15 **mation security needs of the United**
16 **States.**

17 **[[SEC. 502. FAILURE TO NEGOTIATE.**

18 **[[The President may consider a govern-**
19 **ment's refusal to negotiate mutual recogni-**
20 **tion agreements described in section 501**
21 **when considering the participation of the**
22 **United States in any cooperation or assist-**
23 **ance program with that country.**

1 **[[SEC. 503. REPORT TO CONGRESS.**

2 **[[(a) REPORT TO CONGRESS.—The Presi-**
3 **dent shall report annually to the Congress on**
4 **the status of the international effort outlined**
5 **by section 501.**

6 **[[(b) FIRST REPORT.—The first report re-**
7 **quired under subsection (a) shall be submit-**
8 **ted in unclassified form no later than Decem-**
9 **ber 15, 1998.**

10 **[[TITLE VI—MISCELLANEOUS**
11 **PROVISIONS**

12 **[[SEC. 601. EFFECT ON LAW ENFORCEMENT ACTIVITIES.**

13 **[[(a) COLLECTION OF INFORMATION BY AT-**
14 **TORNEY GENERAL.—The Attorney General shall**
15 **compile, and maintain in classified form, data**
16 **on the instances in which encryption has**
17 **interfered with, impeded, or obstructed the**
18 **ability of the Department of Justice to enforce**
19 **the criminal laws of the United States.**

20 **[[(b) AVAILABILITY OF INFORMATION TO THE**
21 **CONGRESS.—The information compiled under**
22 **subsection (a), including an unclassified sum-**
23 **mary thereof, shall be made available, upon**
24 **request, to any Member of Congress.**

1 **[[SEC. 602. INTERPRETATION.**

2 **[[Nothing contained in this Act or the**
3 **amendments made by this Act shall be**
4 **deemed to—**

5 **[[(1) preempt or otherwise affect the**
6 **application of the Arms Export Control**
7 **Act (22 U.S.C. 2751 et seq.), the Export**
8 **Administration Act of 1979 (50 U.S.C. App.**
9 **2401 et seq.), or the International Emer-**
10 **gency Economic Powers Act (50 U.S.C.**
11 **1701 et seq.) or any regulations promul-**
12 **gated thereunder;**

13 **[[(2) affect foreign intelligence activi-**
14 **ties of the United States; or**

15 **[[(3) negate or diminish any intellec-**
16 **tual property protections under the laws**
17 **of the United States or of any State.**

18 **[[SEC. 603. SEVERABILITY.**

19 **[[If any provision of this Act or the**
20 **amendments made by this Act, or the applica-**
21 **tion thereof, to any person or circumstances**
22 **is held invalid by a court of the United States,**
23 **the remainder of this Act or such amend-**
24 **ments, and the application thereof, to other**
25 **persons or circumstances shall not be affected**
26 **thereby.]]**

1 *(SECTION 1. SHORT TITLE.*

2 *(This Act may be cited as the “Security*
 3 *and Freedom Through Encryption (SAFE)*
 4 *Act”.*

5 *(SEC. 2. SALE AND USE OF ENCRYPTION.*

6 *((a) IN GENERAL.—Part I of title 18, United*
 7 *States Code, is amended by inserting after*
 8 *chapter 123 the following new chapter:*

9 *(“CHAPTER 125—ENCRYPTED WIRE AND*
 10 *ELECTRONIC INFORMATION*

(“2801. Definitions.

(“2802. Assistance for law enforcement.

(“2803. Freedom to sell encryption.

(“2804. Prohibition on mandatory key escrow.

(“2805. Unlawful use of encryption in furtherance of a criminal
act.

(“2806. Liability limitations.

11 *(“§ 2801. Definitions*

12 *(“As used in this chapter—*

13 *(“(1) the terms ‘person’, ‘State’, ‘wire*
 14 *communication’, ‘electronic communica-*
 15 *tion’, and ‘investigative or law enforce-*
 16 *ment officer’ have the meanings given*
 17 *those terms in section 2510 of this title;*

18 *(“(2) the terms ‘encrypt’ and*
 19 *‘encryption’ refer to the scrambling of*
 20 *wire communications, electronic commu-*
 21 *nications, or electronically stored infor-*
 22 *mation, using mathematical formulas or*

1 *algorithms in order to preserve the con-*
2 *fidentiality, integrity, or authenticity of,*
3 *and prevent unauthorized recipients from*
4 *accessing or altering, such communica-*
5 *tions or information;*

6 *(“(3) the term ‘key’ means the variable*
7 *information used in a mathematical for-*
8 *mula, code, or algorithm, or any compo-*
9 *nent thereof, used to decrypt wire commu-*
10 *nications, electronic communications, or*
11 *electronically stored information, that*
12 *has been encrypted; and*

13 *(“(4) the term ‘United States person’*
14 *means—*

15 *(“(A) any United States citizen;*

16 *(“(B) any other person organized*
17 *under the laws of any State; and*

18 *(“(C) any person organized under*
19 *the laws of any foreign country who is*
20 *owned or controlled by individuals or*
21 *persons described in subparagraphs*
22 *(A) and (B).*

23 *(“§2802. Assistance for law enforcement*

24 *(“(a) NATIONAL ELECTRONIC TECHNOLOGIES*
25 *CENTER.—*

1 ***“(1) ESTABLISHMENT.—There is estab-***
 2 ***lished in the Department of Justice a Na-***
 3 ***tional Electronic Technologies Center (in***
 4 ***this subsection referred to as the ‘NET***
 5 ***Center’).***

6 ***“(2) DIRECTOR.—The NET Center***
 7 ***shall have a Director, who shall be ap-***
 8 ***pointed by the Attorney General.***

9 ***“(3) DUTIES.—The duties of the NET***
 10 ***Center shall be—***

11 ***“(A) to serve as a center for Fed-***
 12 ***eral, State, and local law enforcement***
 13 ***authorities for information and as-***
 14 ***sistance regarding decryption and***
 15 ***other access requirements;***

16 ***“(B) to serve as a center for in-***
 17 ***dustry and government entities to ex-***
 18 ***change information and methodology***
 19 ***regarding information security tech-***
 20 ***niques and technologies;***

21 ***“(C) to examine encryption tech-***
 22 ***niques and methods to facilitate the***
 23 ***ability of law enforcement to gain effi-***
 24 ***cient access to plaintext of commu-***
 25 ***nications and electronic information;***

1 ***(“(D) to conduct research to de-***
2 ***velop efficient methods, and improve***
3 ***the efficiency of existing methods, of***
4 ***accessing plaintext of communica-***
5 ***tions and electronic information;***

6 ***(“(E) to investigate and research***
7 ***new and emerging techniques and***
8 ***technologies to facilitate access to***
9 ***communications and electronic infor-***
10 ***mation, including —***

11 ***(“(i) reverse-steganography;***

12 ***(“(ii) decompression of infor-***
13 ***mation that previously has been***
14 ***compressed for transmission; and***

15 ***(“(iii) de-multiplexing; and***

16 ***(“(F) to obtain information re-***
17 ***garding the most current hardware,***
18 ***software, telecommunications, and***
19 ***other capabilities to understand how***
20 ***to access information transmitted***
21 ***across networks.***

22 ***(“(4) EQUAL ACCESS.—State and local***
23 ***law enforcement agencies and authorities***
24 ***shall have access to information, services,***
25 ***resources, and assistance provided by the***

1 *NET Center to the same extent that Fed-*
2 *eral law enforcement agencies and au-*
3 *thorities have such access.*

4 ***(“(5) PERSONNEL.—The Director may***
5 ***appoint such personnel as the Director***
6 ***considers appropriate to carry out the du-***
7 ***ties of the NET Center.***

8 ***(“(6) ASSISTANCE OF OTHER FEDERAL***
9 ***AGENCIES.—Upon the request of the Direc-***
10 ***tor of the NET Center, the head of any de-***
11 ***partment or agency of the Federal Govern-***
12 ***ment may, to assist the NET Center in car-***
13 ***rying out its duties under this sub-***
14 ***section—***

15 ***(“(A) detail, on a reimbursable***
16 ***basis, any of the personnel of such de-***
17 ***partment or agency to the NET Cen-***
18 ***ter; and***

19 ***(“(B) provide to the NET Center***
20 ***facilities, information, and other non-***
21 ***personnel resources.***

22 ***(“(7) PRIVATE INDUSTRY ASSISTANCE.—***
23 ***The NET Center may accept, use, and dis-***
24 ***pose of gifts, bequests, or devises of money,***
25 ***services, or property, both real and per-***

1 *sonal, for the purpose of aiding or facili-*
 2 *tating the work of the Center. Gifts, be-*
 3 *quests, or devises of money and proceeds*
 4 *from sales of other property received as*
 5 *gifts, bequests, or devises shall be depos-*
 6 *ited in the Treasury and shall be avail-*
 7 *able for disbursement upon order of the*
 8 *Director of the NET Center.*

9 **(“(8) ADVISORY BOARD.—**

10 **(“(A) ESTABLISHMENT.—***There is es-*
 11 *tablished the Advisory Board of the*
 12 *Strategic NET Center for Excellence*
 13 *in Information Security (in this para-*
 14 *graph referred to as the ‘Advisory*
 15 *Board’), which shall be comprised of*
 16 *members who have the qualifications*
 17 *described in subparagraph (B) and*
 18 *who are appointed by the Attorney*
 19 *General. The Attorney General shall*
 20 *appoint a chairman of the Advisory*
 21 *Board.*

22 **(“(B) QUALIFICATIONS.—***Each mem-*
 23 *ber of the Advisory Board shall have*
 24 *experience or expertise in the field of*
 25 *encryption, decryption, electronic com-*

1 *munication, information security,*
2 *electronic commerce, or law enforce-*
3 *ment.*

4 ***“(C) DUTIES.—The duty of the Ad-***
5 ***visory Board shall be to advise the***
6 ***NET Center and the Federal Govern-***
7 ***ment regarding new and emerging***
8 ***technologies relating to encryption***
9 ***and decryption of communications***
10 ***and electronic information.***

11 ***“(9) IMPLEMENTATION PLAN.—Within 2***
12 ***months after the date of the enactment of***
13 ***the Security and Freedom Through***
14 ***Encryption (SAFE) Act, the Attorney Gen-***
15 ***eral shall, in consultation and coopera-***
16 ***tion with other appropriate Federal agen-***
17 ***cies and appropriate industry partici-***
18 ***pants, develop and cause to be published***
19 ***in the Federal Register a plan for estab-***
20 ***lishing the NET Center. The plan shall—***

21 ***“(A) specify the physical location***
22 ***of the NET Center and the equipment,***
23 ***software, and personnel resources nec-***
24 ***essary to carry out the duties of the***
25 ***NET Center under this subsection;***

1 ***(“(B) assess the amount of fund-***
2 ***ing necessary to establish and operate***
3 ***the NET Center; and***

4 ***(“(C) identify sources of probable***
5 ***funding for the NET Center, including***
6 ***any sources of in-kind contributions***
7 ***from private industry.***

8 ***(“(b) FREEDOM OF USE.—Subject to section***
9 ***2805, it shall be lawful for any person within***
10 ***any State, and for any United States person in***
11 ***a foreign country, to use any encryption, re-***
12 ***gardless of the encryption algorithm selected,***
13 ***encryption key length chosen, or implementa-***
14 ***tion technique or medium used. No Federal or***
15 ***State law or regulation may condition the is-***
16 ***suance of certificates of authentication or cer-***
17 ***tificates of authority for any encryption prod-***
18 ***uct upon any escrowing or other sharing of***
19 ***private encryption keys, whether with private***
20 ***agents or government entities, or establish a li-***
21 ***censing, labeling, or other regulatory scheme***
22 ***for any encryption product that requires key***
23 ***escrow as a condition of licensing or regu-***
24 ***latory approval.***

1 *(“§2803. Freedom to sell encryption*

2 *(“Subject to section 2805, it shall be lawful*
 3 *for any person within any State to sell in inter-*
 4 *state commerce any encryption, regardless of*
 5 *the encryption algorithm selected, encryption*
 6 *key length chosen, or implementation tech-*
 7 *nique or medium used.*

8 *(“§2804. Prohibition on mandatory key escrow*

9 *(“(a) PROHIBITION.—No person in lawful*
 10 *possession of a key to encrypted communica-*
 11 *tions or information may be required by Fed-*
 12 *eral or State law to relinquish to another per-*
 13 *son control of that key.*

14 *(“(b) EXCEPTION FOR ACCESS FOR LAW EN-*
 15 *FORCEMENT PURPOSES.—Subsection (a) shall*
 16 *not affect the authority of any investigative or*
 17 *law enforcement officer, or any member of the*
 18 *intelligence community as defined in section 3*
 19 *of the National Security Act of 1947 (50 U.S.C.*
 20 *401a), acting under any law in effect on the ef-*
 21 *fective date of this chapter, to gain access to*
 22 *encrypted communications or information.*

23 *(“§2805. Unlawful use of encryption in furtherance of*
 24 *a criminal act*

25 *(“Any person who, in the commission of a*
 26 *felony under a criminal statute of the United*

1 *States, knowingly and willfully encrypts in-*
2 *criminating communications or information*
3 *relating to that felony with the intent to con-*
4 *ceal such communications or information for*
5 *the purpose of avoiding detection by law en-*
6 *forcement agencies or prosecution—*

7 *(“(1) in the case of a first offense*
8 *under this section, shall be imprisoned for*
9 *not more than 10 years, or fined in the*
10 *amount set forth in this title, or both; and*

11 *(“(2) in the case of a second or subse-*
12 *quent offense under this section, shall be*
13 *imprisoned for not more than 20 years, or*
14 *fined in the amount set forth in this title,*
15 *or both.*

16 *(“§2806. Liability limitations*

17 *(“No person shall be subject to civil or*
18 *criminal liability for providing access to the*
19 *plaintext of encrypted communications or elec-*
20 *tronic information to any law enforcement of-*
21 *ficial or authorized government entity, pursu-*
22 *ant to judicial process.”.*

23 *((b) STUDY.—Within 6 months after the*
24 *date of the enactment of this Act, the National*
25 *Telecommunications and Information Admin-*

1 *istration shall conduct a study, and prepare*
 2 *and submit to the Congress and the President*
 3 *a report regarding such study, that—*

4 *((1) assesses the effect that establish-*
 5 *ment of a mandatory system for recovery*
 6 *of encryption keys for encrypted commu-*
 7 *nications and information would have*
 8 *on—*

9 *((A) electronic commerce;*

10 *((B) data security;*

11 *((C) privacy in interstate com-*
 12 *merce; and*

13 *((D) law enforcement authorities*
 14 *and activities; and*

15 *((2) assesses other possible methods*
 16 *for providing access to encrypted commu-*
 17 *nications and information to further law*
 18 *enforcement activities.*

19 *((c) CONFORMING AMENDMENT.—The table*
 20 *of chapters for part I of title 18, United States*
 21 *Code, is amended by inserting after the item*
 22 *relating to chapter 123 the following new item:*

“125. Encrypted wire and electronic information 2801”.

23 *(SEC. 3. EXPORTS OF ENCRYPTION.*

24 *((a) AMENDMENT TO EXPORT ADMINISTRA-*
 25 *TION ACT OF 1979.—Section 17 of the Export Ad-*

1 *ministration Act of 1979 (50 U.S.C. App. 2416)*
2 *is amended by adding at the end thereof the*
3 *following new subsection:*

4 ***(“(g) COMPUTERS AND RELATED EQUIP-***
5 ***MENT.—***

6 ***(“(1) GENERAL RULE.—Subject to para-***
7 ***graphs (2), (3), and (4), the Secretary***
8 ***shall have exclusive authority to control***
9 ***exports of all computer hardware, soft-***
10 ***ware, and technology for information se-***
11 ***curity (including encryption), except that***
12 ***which is specifically designed or modified***
13 ***for military use, including command, con-***
14 ***trol, and intelligence applications.***

15 ***(“(2) ITEMS NOT REQUIRING LICENSES.—***
16 ***No validated license may be required, ex-***
17 ***cept pursuant to the Trading With The***
18 ***Enemy Act or the International Emer-***
19 ***gency Economic Powers Act (but only to***
20 ***the extent that the authority of such Act is***
21 ***not exercised to extend controls imposed***
22 ***under this Act), for the export or reexport***
23 ***of—***

24 ***(“(A) any software, including soft-***
25 ***ware with encryption capabilities—***

1 *(“(i) that is generally avail-*
2 *able, as is, and is designed for in-*
3 *stallation by the purchaser; or*

4 *(“(ii) that is in the public do-*
5 *main for which copyright or other*
6 *protection is not available under*
7 *title 17, United States Code, or*
8 *that is available to the public be-*
9 *cause it is generally accessible to*
10 *the interested public in any form;*
11 *or*

12 *(“(B) any computing device solely*
13 *because it incorporates or employs in*
14 *any form software (including software*
15 *with encryption capabilities) exempt-*
16 *ed from any requirement for a vali-*
17 *dated license under subparagraph*
18 *(A).*

19 *(“(3) SOFTWARE WITH ENCRYPTION CAPA-*
20 *BILITIES.—The Secretary shall authorize*
21 *the export or reexport of software with*
22 *encryption capabilities for nonmilitary*
23 *end uses in any country to which exports*
24 *of software of similar capability are per-*
25 *mitted for use by financial institutions*

1 *not controlled in fact by United States*
2 *persons, unless there is substantial evi-*
3 *dence that such software will be—*

4 *“(A) diverted to a military end*
5 *use or an end use supporting inter-*
6 *national terrorism;*

7 *“(B) modified for military or ter-*
8 *rorist end use; or*

9 *“(C) reexported without any au-*
10 *thorization by the United States that*
11 *may be required under this Act.*

12 *“(4) HARDWARE WITH ENCRYPTION CA-*
13 *PABILITIES.—The Secretary shall authorize*
14 *the export or reexport of computer hard-*
15 *ware with encryption capabilities if the*
16 *Secretary determines that a product offer-*
17 *ing comparable security is commercially*
18 *available outside the United States from a*
19 *foreign supplier, without effective restric-*
20 *tions.*

21 *“(5) DEFINITIONS.—As used in this*
22 *subsection—*

23 *“(A) the term ‘encryption’ means*
24 *the scrambling of wire or electronic*
25 *information using mathematical for-*

1 *mulas or algorithms in order to pre-*
2 *serve the confidentiality, integrity, or*
3 *authenticity of, and prevent unauthor-*
4 *ized recipients from accessing or al-*
5 *tering, such information;*

6 *“(B) the term ‘generally avail-*
7 *able’ means, in the case of software*
8 *(including software with encryption*
9 *capabilities), software that is offered*
10 *for sale, license, or transfer to any*
11 *person without restriction, whether or*
12 *not for consideration, including, but*
13 *not limited to, over-the-counter retail*
14 *sales, mail order transactions, phone*
15 *order transactions, electronic dis-*
16 *tribution, or sale on approval;*

17 *“(C) the term ‘as is’ means, in the*
18 *case of software (including software*
19 *with encryption capabilities), a soft-*
20 *ware program that is not designed,*
21 *developed, or tailored by the software*
22 *publisher for specific purchasers, ex-*
23 *cept that such purchasers may supply*
24 *certain installation parameters need-*
25 *ed by the software program to func-*

1 *tion properly with the purchaser's sys-*
2 *tem and may customize the software*
3 *program by choosing among options*
4 *contained in the software program;*

5 *(“(D) the term ‘is designed for in-*
6 *stallation by the purchaser’ means, in*
7 *the case of software (including soft-*
8 *ware with encryption capabilities)*
9 *that—*

10 *(“(i) the software publisher in-*
11 *tends for the purchaser (including*
12 *any licensee or transferee), who*
13 *may not be the actual program*
14 *user, to install the software pro-*
15 *gram on a computing device and*
16 *has supplied the necessary in-*
17 *structions to do so, except that the*
18 *publisher may also provide tele-*
19 *phone help line services for soft-*
20 *ware installation, electronic*
21 *transmission, or basic operations;*
22 *and*

23 *(“(ii) the software program is*
24 *designed for installation by the*

1 *purchaser without further sub-*
2 *stantial support by the supplier;*

3 *(“(E) the term ‘computing device’*
4 *means a device which incorporates*
5 *one or more microprocessor-based*
6 *central processing units that can ac-*
7 *cept, store, process, or provide output*
8 *of data; and*

9 *(“(F) the term ‘computer hard-*
10 *ware’, when used in conjunction with*
11 *information security, includes, but is*
12 *not limited to, computer systems,*
13 *equipment, application-specific as-*
14 *semblies, modules, and integrated cir-*
15 *cuits.”.*

16 *((b) CONTINUATION OF EXPORT ADMINISTRA-*
17 *TION ACT.—For purposes of carrying out the*
18 *amendment made by subsection (a), the Export*
19 *Administration Act of 1979 shall be deemed to*
20 *be in effect.*

21 *(SEC. 4. TREATMENT OF ENCRYPTION IN INTERSTATE AND*
22 *FOREIGN COMMERCE.*

23 *((a) INQUIRY REGARDING IMPEDIMENTS TO*
24 *TRADE.—Within 180 days after the date of the*

1 *enactment of this Act, the Secretary of Com-*
2 *merce shall complete an inquiry to—*

3 *((1) identify any domestic and foreign*
4 *impediments to trade in encryption prod-*
5 *ucts and services and the manners in*
6 *which and extent to which such impedi-*
7 *ments inhibit the development of inter-*
8 *state and foreign commerce; and*

9 *((2) identify import restrictions im-*
10 *posed by foreign nations that constitute*
11 *unfair trade barriers to providers of*
12 *encryption products or services.*

13 *The Secretary shall submit a report to the Con-*
14 *gress regarding the results of such inquiry by*
15 *such date.*

16 *((b) REMOVAL OF IMPEDIMENTS TO TRADE.—*
17 *Within 1 year after such date of enactment, the*
18 *Secretary of Commerce, in consultation with*
19 *the Attorney General, shall prescribe such reg-*
20 *ulations as may be necessary to reduce the im-*
21 *pediments to trade in encryption products and*
22 *services identified in the inquiry pursuant to*
23 *subsection (a) for the purpose of facilitating*
24 *the development of interstate and foreign com-*
25 *merce. Such regulations shall be designed to—*

1 ***((1) promote the sale and distribution***
2 ***in foreign commerce of encryption prod-***
3 ***ucts and services manufactured in the***
4 ***United States; and***

5 ***((2) strengthen the competitiveness of***
6 ***domestic providers of encryption products***
7 ***and services in foreign commerce.***

8 ***((c) INTERNATIONAL AGREEMENTS.—***

9 ***((1) REPORT TO PRESIDENT.—Upon the***
10 ***completion of the inquiry under sub-***
11 ***section (a), the Secretary of Commerce***
12 ***shall submit a report to the President re-***
13 ***garding reducing any impediments to***
14 ***trade in encryption products and services***
15 ***that are identified by the inquiry and***
16 ***could, in the determination of the Sec-***
17 ***retary, require international negotiations***
18 ***for such reduction.***

19 ***((2) NEGOTIATIONS.—The President***
20 ***shall take all actions necessary to con-***
21 ***duct negotiations with other countries for***
22 ***the purposes of (A) concluding inter-***
23 ***national agreements on the promotion of***
24 ***encryption products and services, and (B)***
25 ***achieving mutual recognition of coun-***

1 *tries' export controls, in order to meet the*
2 *needs of countries to preserve national se-*
3 *curity, safeguard privacy, and prevent*
4 *commercial espionage. The President may*
5 *consider a country's refusal to negotiate*
6 *such international export and mutual rec-*
7 *ognition agreements when considering the*
8 *participation of the United States in any*
9 *cooperation or assistance program with*
10 *that country. The President shall submit*
11 *a report to the Congress regarding the*
12 *status of international efforts regarding*
13 *cryptography not later than December 31,*
14 *2000.*

15 ***((d) DEFINITIONS.—For purposes of this***
16 ***section, the following definitions shall apply:***

17 ***((1) COMMUNICATION.—The term “com-***
18 ***munication” includes wire communica-***
19 ***tion and electronic communication.***

20 ***((2) DECRYPT; DECRYPTION.—The terms***
21 ***“decrypt” and “decryption” refer to the***
22 ***electronic retransformation of commu-***
23 ***nications or electronically stored informa-***
24 ***tion that has been encrypted into the***

1 *original form of the communication or in-*
2 *formation.*

3 ***((3) ELECTRONIC COMMUNICATION.—The***
4 ***term “electronic communication” has the***
5 ***meaning given such term in section 2510***
6 ***of title 18, United States Code.***

7 ***((4) ENCRYPT; ENCRYPTION.—The terms***
8 ***“encrypt” and “encryption” have the***
9 ***meanings given such terms in section 2801***
10 ***of title 18, United States Code (as added***
11 ***by section 2 of this Act).***

12 ***((5) ENCRYPTION PRODUCT.—The term***
13 ***“encryption product” means any product,***
14 ***software, or technology that can be used***
15 ***to encrypt and decrypt communications or***
16 ***electronic information and any product,***
17 ***software, or technology with encryption***
18 ***capabilities;***

19 ***((6) WIRE COMMUNICATION.—The term***
20 ***“wire communication” has the meaning***
21 ***given such term in section 3 of the Com-***
22 ***munications Act of 1934 (47 U.S.C. 153).***

23 ***(SEC. 5. EFFECT ON LAW ENFORCEMENT ACTIVITIES.***

24 ***((a) COLLECTION OF INFORMATION BY AT-***
25 ***TORNEY GENERAL.—The Attorney General shall***

1 *compile, and maintain in classified form, data*
2 *on the instances in which encryption (as de-*
3 *fin ed in section 2801 of title 18, United States*
4 *Code) has interfered with, impeded, or ob-*
5 *structed the ability of the Department of Jus-*
6 *tice to enforce the criminal laws of the United*
7 *States.*

8 ***((b) AVAILABILITY OF INFORMATION TO THE***
9 ***CONGRESS.—The information compiled under***
10 ***subsection (a), including an unclassified sum-***
11 ***mary thereof, shall be made available, upon***
12 ***request, to any Member of Congress.)***

Amend the title so as to read: “A bill to amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption.”.