

Union Calendar No. 149

106<sup>TH</sup> CONGRESS  
1<sup>ST</sup> Session

**H. R. 850**

[Report No. 106-117, 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.

---

JULY 23, 1999

Reported from the Committee on Armed Services with  
amendments

JULY 23, 1999

Reported from the Permanent Select Committee on Intelligence 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. 149

106TH CONGRESS  
1ST SESSION

# H. R. 850

**[Report No. 106–117, 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 25, 1999

Mr. GOODLATTE (for himself, Ms. LOFGREN, Mr. ARMEY, Mr. DELAY, Mr. WATTS of Oklahoma, Mr. DAVIS of Virginia, Mr. COX, Ms. PRYCE of Ohio, Mr. BLUNT, Mr. GEPHARDT, Mr. BONIOR, Mr. FROST, Ms. DELAURO, Mr. LEWIS of Georgia, Mr. GEJDENSON, Mr. SENSENBRENNER, Mr. GEKAS, Mr. COBLE, Mr. SMITH of Texas, Mr. GALLEGLY, Mr. BRYANT, Mr. CHABOT, Mr. BARR of Georgia, Mr. HUTCHINSON, Mr. PEASE, Mr. CANNON, Mr. ROGAN, Mrs. BONO, Mr. BACHUS, Mr. CONYERS, Mr. FRANK of Massachusetts, Mr. BOUCHER, Mr. NADLER, Ms. JACKSON-LEE of Texas, Ms. WATERS, Mr. MEEHAN, Mr. DELAHUNT, Mr. WEXLER, Mr. ACKERMAN, Mr. ANDREWS, Mr. ARCHER, Mr. BALLENGER, Mr. BARCIA, Mr. BARRETT of Nebraska, Mr. BARRETT of Wisconsin, Mr. BARTON of Texas, Mr. BILBRAY, Mr. BLUMENAUER, Mr. BOEHNER, Mr. BRADY of Texas, Mr. BRADY of Pennsylvania, Ms. BROWN of Florida, Mr. BROWN of California, Mr. BURR of North Carolina, Mr. BURTON of Indiana, Mr. CAMP, Mr. CAMPBELL, Mrs. CAPPS, Mr. CHAMBLISS, Mrs. CHENOWETH, Mrs. CHRISTIAN-CHRISTENSEN, Mrs. CLAYTON, Mr. CLEMENT, Mr. CLYBURN, Mr. COLLINS, Mr. COOK, Mr. COOKSEY, Mrs. CUBIN, Mr. CUMMINGS, Mr. CUNNINGHAM, Mr. DAVIS of Illinois, Mr. DEAL of Georgia, Mr. DEFazio, Mr. DEUTSCH, Mr. DICKEY, Mr. DOOLEY of California, Mr. DOOLITTLE, Mr. DOYLE, Mr. DREIER, Mr. DUNCAN, Ms. DUNN, Mr. EHLERS, Mrs. EMERSON, Mr. ENGLISH, Ms. ESHOO, Mr. EWING, Mr. FARR of California, Mr. FILLNER, Mr. FORD, Mr. FOSSELLA, Mr. FRANKS of New Jersey, Mr. GILLMOR, Mr. GOODE, Mr. GOODLING, Mr. GORDON, Mr. GREEN of Texas, Mr. GUTKNECHT, Mr. HALL of Texas, Mr. HASTINGS of Washington, Mr. HERGER, Mr. HILL of Montana, Mr. HOBSON, Mr. HOEKSTRA, Mr. HOLDEN, Ms. HOOLEY of Oregon, Mr. HORN, Mr. HOUGH-

TON, Mr. INSLEE, Mr. ISTOOK, Mr. JACKSON of Illinois, Mr. JEFFERSON, Ms. EDDIE BERNICE JOHNSON of Texas, Mrs. JOHNSON of Connecticut, Mr. KANJORSKI, Mr. KASICH, Mrs. KELLY, Ms. KIKPATRICK, Mr. KIND, Mr. KINGSTON, Mr. KNOLLENBERG, Mr. KOLBE, Mr. LAMPSON, Mr. LARGENT, Mr. LATHAM, Ms. LEE, Mr. LEWIS of Kentucky, Mr. LINDER, Mr. LUCAS of Oklahoma, Mr. LUTHER, Ms. MCCARTHY of Missouri, Mr. McDERMOTT, Mr. MCGOVERN, Mr. MCINTOSH, Mr. MALONEY of Connecticut, Mr. MANZULLO, Mr. MARKEY, Mr. MARTINEZ, Mr. MATSUI, Mrs. MEEK of Florida, Mr. METCALF, Mr. MICA, Ms. MILLENDER-MCDONALD, Mr. GEORGE MILLER of California, Mr. MOAKLEY, Mr. MORAN of Virginia, Mrs. MORELLA, Mrs. MYRICK, Mrs. NAPOLITANO, Mr. NEAL of Massachusetts, Mr. NETHERCUTT, Mr. NORWOOD, Mr. NUSSLE, Mr. OLVER, Mr. PACKARD, Mr. PALLONE, Mr. PASTOR, Mr. PETERSON of Minnesota, Mr. PICKERING, Mr. POMBO, Mr. POMEROY, Mr. PRICE of North Carolina, Mr. QUINN, Mr. RADANOVICH, Mr. RAHALL, Mr. RANGEL, Mr. REYNOLDS, Ms. RIVERS, Mr. ROHRBACHER, Ms. ROS-LEHTINEN, Mr. RUSH, Mr. SALMON, Ms. SANCHEZ, Mr. SANDERS, Mr. SANFORD, Mr. SCARBOROUGH, Mr. SCHAFFER, Mr. SESSIONS, Mr. SHAYS, Mr. SHERMAN, Mr. SHIMKUS, Mr. SMITH of Washington, Mr. SMITH of New Jersey, Mr. SOUDER, Ms. STABENOW, Mr. STARK, Mr. SUNUNU, Mr. TANNER, Mrs. TAUSCHER, Mr. TAUZIN, Mr. TAYLOR of North Carolina, Mr. THOMAS, Mr. THOMPSON of Mississippi, Mr. THUNE, Mr. TIAHRT, Mr. TIERNEY, Mr. UPTON, Mr. VENTO, Mr. WALSH, Mr. WAMP, Mr. WATKINS, Mr. WELLER, Mr. WHITFIELD, Mr. WICKER, Ms. WOOLSEY, and Mr. WU) 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

APRIL 27, 1999

Reported from the Committee on the Judiciary

APRIL 27, 1999

Referral to the Committee on International Relations extended for a period ending not later than July 2, 1999

APRIL 27, 1999

Referred to the Committees on Armed Services and Commerce and the Permanent Select Committee on Intelligence for a period ending not later than July 2, 1999

JULY 2, 1999

Reported from the Committee on Commerce with an amendment

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

JULY 2, 1999

Referral to the Committee on International Relations extended for a period ending not later than July 16, 1999

JULY 2, 1999

Referral to the Committee on Armed Services and the Permanent Select Committee on Intelligence extended for a period ending not later than July 23, 1999

JULY 16, 1999

Referral to the Committee on International Relations extended for a period ending not later than July 19, 1999

JULY 19, 1999

Reported from the Committee on International Relations with an amendment  
[Strike out all after the enacting clause and insert the part printed in boldface roman]

JULY 23, 1999

Reported from the Committee on Armed Services with amendments  
[Strike out all after the enacting clause and insert the part printed in italic and bold brackets]

JULY 23, 1999

Additional sponsors: Mr. HALL of Ohio, Mr. FORBES, Mr. HOLT, Mr. GIBBONS, Mr. CALVERT, Ms. SLAUGHTER, Mr. BONILLA, Mr. DIAZ-BALART, Mr. ENGEL, Mr. HILLIARD, Mr. KING, Mr. LAHOOD, Ms. MCKINNEY, Mr. NEY, Mrs. NORTHUP, Mr. RILEY, Mr. SERRANO, Mr. STENHOLM, Mr. TANCREDO, Mr. HANSEN, Mr. MORAN of Kansas, Mr. SAM JOHNSON of Texas, Mr. HILLEARY, Mr. GARY MILLER of California, Ms. NORTON, Mr. SWEENEY, Mr. BAKER, Mr. CRANE, Mr. MCINNIS, Mr. WELDON of Florida, Mr. WISE, Mr. OSE, Mr. BALDACCI, Mr. MINGE, Mr. UNDERWOOD, Mr. DEMINT, Mr. WALDEN of Oregon, Mr. HAYES, Mr. FOLEY, Mr. TERRY, Mr. SHOWS, Mr. RYAN of Wisconsin, Mr. ETHERIDGE, Mr. WATT of North Carolina, Mr. CROWLEY, Mr. UDALL of Colorado, Mr. HOEFFEL, Mr. FLETCHER, Mr. BAIRD, Mr. TALENT, Mr. KENNEDY of Rhode Island, Mr. UDALL of New Mexico, Mr. SAWYER, Mr. MENENDEZ, and Mr. HINCHEY

Deleted sponsors: Mr. HOLDEN (added February 25, 1999; deleted April 21, 1999), and Mr. HASTINGS of Florida (added March 16, 1999; deleted June 10, 1999)

JULY 23, 1999

Reported from the Permanent Select Committee on Intelligence 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]

---

## 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 123 the fol-  
9 lowing new chapter:

10 **“CHAPTER 125—ENCRYPTED WIRE AND**  
11 **ELECTRONIC INFORMATION**

“Sec.

“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.

12 **“§ 2801. Definitions**

13 “As used in this chapter—

14 “(1) the terms ‘person’, ‘State’, ‘wire commu-  
15 nication’, ‘electronic communication’, ‘investigative  
16 or law enforcement officer’, and ‘judge of competent  
17 jurisdiction’ have the meanings given those terms in  
18 section 2510 of this title;

1           “(2) the term ‘decrypt’ means to retransform or  
2           unscramble encrypted data, including communica-  
3           tions, to its readable form;

4           “(3) the terms ‘encrypt’, ‘encrypted’, and  
5           ‘encryption’ mean the scrambling of wire commu-  
6           nications, electronic communications, or electroni-  
7           cally stored information, using mathematical for-  
8           mulas or algorithms in order to preserve the con-  
9           fidentiality, integrity, or authenticity of, and prevent  
10          unauthorized recipients from accessing or altering,  
11          such communications or information;

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

18          “(5) the term ‘key recovery information’ means  
19          information that would enable obtaining the key of  
20          a user of encryption;

21          “(6) the term ‘plaintext access capability’  
22          means any method or mechanism which would pro-  
23          vide information in readable form prior to its being  
24          encrypted or after it has been decrypted;

25          “(7) the term ‘United States person’ means—

1           “(A) any United States citizen;

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

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

10 **“§ 2802. Freedom to use encryption**

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

16 **“§ 2803. Freedom to sell encryption**

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

22 **“§ 2804. Prohibition on mandatory key escrow**

23       “(a) GENERAL PROHIBITION.—Neither the Federal  
24 Government nor a State may require that, or condition  
25 any approval on a requirement that, a key, access to a

1 key, key recovery information, or any other plaintext ac-  
2 cess capability be—

3           “(1) built into computer hardware or software  
4 for any purpose;

5           “(2) given to any other person, including a  
6 Federal Government agency or an entity in the pri-  
7 vate sector that may be certified or approved by the  
8 Federal Government or a State to receive it; or

9           “(3) retained by the owner or user of an  
10 encryption key or any other person, other than for  
11 encryption products for use by the Federal Govern-  
12 ment or a State.

13           “(b) PROHIBITION ON LINKAGE OF DIFFERENT  
14 USES OF ENCRYPTION.—Neither the Federal Government  
15 nor a State may—

16           “(1) require the use of encryption products,  
17 standards, or services used for confidentiality pur-  
18 poses, as a condition of the use of such products,  
19 standards, or services for authenticity or integrity  
20 purposes; or

21           “(2) require the use of encryption products,  
22 standards, or services used for authenticity or integ-  
23 rity purposes, as a condition of the use of such prod-  
24 ucts, standards, or services for confidentiality pur-  
25 poses.

1       “(c) EXCEPTION FOR ACCESS FOR LAW ENFORCE-  
2       MENT PURPOSES.—Subsection (a) shall not affect the au-  
3       thority of any investigative or law enforcement officer, or  
4       any member of the intelligence community as defined in  
5       section 3 of the National Security Act of 1947 (50 U.S.C.  
6       401a), acting under any law in effect on the effective date  
7       of this chapter, to gain access to encrypted communica-  
8       tions or information.

9       **“§ 2805. Unlawful use of encryption in furtherance of**  
10                                   **a criminal act**

11       “(a) ENCRYPTION OF INCRIMINATING COMMUNICA-  
12       TIONS OR INFORMATION UNLAWFUL.—Any person who,  
13       in the commission of a felony under a criminal statute of  
14       the United States, knowingly and willfully encrypts in-  
15       criminating communications or information relating to  
16       that felony with the intent to conceal such communications  
17       or information for the purpose of avoiding detection by  
18       law enforcement agencies or prosecution—

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

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

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

3 “(b) USE OF ENCRYPTION NOT A BASIS FOR PROB-  
 4 ABLE CAUSE.—The use of encryption by any person shall  
 5 not be the sole basis for establishing probable cause with  
 6 respect to a criminal offense or a search warrant.”.

7 (b) CONFORMING AMENDMENT.—The table of chap-  
 8 ters for part I of title 18, United States Code, is amended  
 9 by inserting after the item relating to chapter 123 the fol-  
 10 lowing new item:

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

11 **SEC. 3. EXPORTS OF ENCRYPTION.**

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

16 “(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS,  
 17 AND RELATED EQUIPMENT.—

18 “(1) GENERAL RULE.—Subject to paragraphs  
 19 (2) and (3), the Secretary shall have exclusive au-  
 20 thority to control exports of all computer hardware,  
 21 software, computing devices, customer premises  
 22 equipment, communications network equipment, and  
 23 technology for information security (including  
 24 encryption), except that which is specifically de-

1 signed or modified for military use, including com-  
2 mand, control, and intelligence applications.

3 “(2) ITEMS NOT REQUIRING LICENSES.—After  
4 a one-time, 15-day technical review by the Secretary,  
5 no export license may be required, except pursuant  
6 to the Trading with the enemy Act or the Inter-  
7 national Emergency Economic Powers Act (but only  
8 to the extent that the authority of such Act is not  
9 exercised to extend controls imposed under this Act),  
10 for the export or reexport of—

11 “(A) any computer hardware or software  
12 or computing device, including computer hard-  
13 ware or software or computing devices with  
14 encryption capabilities—

15 “(i) that is generally available;

16 “(ii) that is in the public domain for  
17 which copyright or other protection is not  
18 available under title 17, United States  
19 Code, or that is available to the public be-  
20 cause it is generally accessible to the inter-  
21 ested public in any form; or

22 “(iii) that is used in a commercial,  
23 off-the-shelf, consumer product or any  
24 component or subassembly designed for  
25 use in such a consumer product available

1 within the United States or abroad  
2 which—

3 “(I) includes encryption capabilities  
4 which are inaccessible to the end  
5 user; and

6 “(II) is not designed for military  
7 or intelligence end use;

8 “(B) any computing device solely because  
9 it incorporates or employs in any form—

10 “(i) computer hardware or software  
11 (including computer hardware or software  
12 with encryption capabilities) that is ex-  
13 emptioned from any requirement for a license  
14 under subparagraph (A); or

15 “(ii) computer hardware or software  
16 that is no more technically complex in its  
17 encryption capabilities than computer  
18 hardware or software that is exemptioned  
19 from any requirement for a license under  
20 subparagraph (A) but is not designed for  
21 installation by the purchaser;

22 “(C) any computer hardware or software  
23 or computing device solely on the basis that it  
24 incorporates or employs in any form interface  
25 mechanisms for interaction with other computer

1 hardware or software or computing devices, in-  
2 cluding computer hardware and software and  
3 computing devices with encryption capabilities;

4 “(D) any computing or telecommunication  
5 device which incorporates or employs in any  
6 form computer hardware or software encryption  
7 capabilities which—

8 “(i) are not directly available to the  
9 end user; or

10 “(ii) limit the encryption to be point-  
11 to-point from the user to a central commu-  
12 nications point or link and does not enable  
13 end-to-end user encryption;

14 “(E) technical assistance and technical  
15 data used for the installation or maintenance of  
16 computer hardware or software or computing  
17 devices with encryption capabilities covered  
18 under this subsection; or

19 “(F) any encryption hardware or software  
20 or computing device not used for confidentiality  
21 purposes, such as authentication, integrity, elec-  
22 tronic signatures, nonrepudiation, or copy pro-  
23 tection.

24 “(3) COMPUTER HARDWARE OR SOFTWARE OR  
25 COMPUTING DEVICES WITH ENCRYPTION CAPABILI-

1 TIES.—After a one-time, 15-day technical review by  
2 the Secretary, the Secretary shall authorize the ex-  
3 port or reexport of computer hardware or software  
4 or computing devices with encryption capabilities for  
5 nonmilitary end uses in any country—

6 “(A) to which exports of computer hard-  
7 ware or software or computing devices of com-  
8 parable strength are permitted for use by finan-  
9 cial institutions not controlled in fact by United  
10 States persons, unless there is substantial evi-  
11 dence that such computer hardware or software  
12 or computing devices will be—

13 “(i) diverted to a military end use or  
14 an end use supporting international ter-  
15 rorism;

16 “(ii) modified for military or terrorist  
17 end use; or

18 “(iii) reexported without any author-  
19 ization by the United States that may be  
20 required under this Act; or

21 “(B) if the Secretary determines that a  
22 computer hardware or software or computing  
23 device offering comparable security is commer-  
24 cially available outside the United States from  
25 a foreign supplier, without effective restrictions.

1           “(4) DEFINITIONS.—As used in this  
2 subsection—

3           “(A)(i) the term ‘encryption’ means the  
4 scrambling of wire communications, electronic  
5 communications, or electronically stored infor-  
6 mation, using mathematical formulas or algo-  
7 rithms in order to preserve the confidentiality,  
8 integrity, or authenticity of, and prevent unau-  
9 thorized recipients from accessing or altering,  
10 such communications or information;

11           “(ii) the terms ‘wire communication’ and  
12 ‘electronic communication’ have the meanings  
13 given those terms in section 2510 of title 18,  
14 United States Code;

15           “(B) the term ‘generally available’ means,  
16 in the case of computer hardware or computer  
17 software (including computer hardware or com-  
18 puter software with encryption capabilities)—

19           “(i) computer hardware or computer  
20 software that is—

21           “(I) distributed through the  
22 Internet;

23           “(II) offered for sale, license, or  
24 transfer to any person without restric-  
25 tion, whether or not for consideration;

1 including, but not limited to, over-the-  
2 counter retail sales, mail order trans-  
3 actions, phone order transactions,  
4 electronic distribution, or sale on ap-  
5 proval;

6 “(III) preloaded on computer  
7 hardware or computing devices that  
8 are widely available for sale to the  
9 public; or

10 “(IV) assembled from computer  
11 hardware or computer software com-  
12 ponents that are widely available for  
13 sale to the public;

14 “(ii) not designed, developed, or tai-  
15 lored by the manufacturer for specific pur-  
16 chasers or users, except that any such pur-  
17 chaser or user may—

18 “(I) supply certain installation  
19 parameters needed by the computer  
20 hardware or software to function  
21 properly with the computer system of  
22 the user or purchaser; or

23 “(II) select from among options  
24 contained in the computer hardware  
25 or computer software; and

1           “(iii) with respect to which the manu-  
2           facturer of that computer hardware or  
3           computer software—

4                   “(I) intended for the user or pur-  
5                   chaser, including any licensee or  
6                   transferee, to install the computer  
7                   hardware or software and has sup-  
8                   plied the necessary instructions to do  
9                   so, except that the manufacturer of  
10                  the computer hardware or software, or  
11                  any agent of such manufacturer, may  
12                  also provide telephone or electronic  
13                  mail help line services for installation,  
14                  electronic transmission, or basic oper-  
15                  ations; and

16                  “(II) the computer hardware or  
17                  software is designed for such installa-  
18                  tion by the user or purchaser without  
19                  further substantial support by the  
20                  manufacturer;

21                  “(C) the term ‘computing device’ means a  
22                  device which incorporates one or more micro-  
23                  processor-based central processing units that  
24                  can accept, store, process, or provide output of  
25                  data;

1           “(D) the term ‘computer hardware’ in-  
2 eludes, but is not limited to, computer systems,  
3 equipment, application-specific assemblies,  
4 smart cards, modules, integrated circuits, and  
5 printed circuit board assemblies;

6           “(E) the term ‘customer premises equip-  
7 ment’ means equipment employed on the prem-  
8 ises of a person to originate, route, or terminate  
9 communications;

10          “(F) the term ‘technical assistance’ in-  
11 eludes instruction, skills training, working  
12 knowledge, consulting services, and the transfer  
13 of technical data;

14          “(G) the term ‘technical data’ includes  
15 blueprints, plans, diagrams, models, formulas,  
16 tables, engineering designs and specifications,  
17 and manuals and instructions written or re-  
18 corded on other media or devices such as disks,  
19 tapes, or read-only memories; and

20          “(H) the term ‘technical review’ means a  
21 review by the Secretary of computer hardware  
22 or software or computing devices with  
23 encryption capabilities, based on information  
24 about the product’s encryption capabilities sup-  
25 plied by the manufacturer, that the computer

1 hardware or software or computing device  
2 works as represented.”.

3 (b) ~~NO REINSTATEMENT OF EXPORT CONTROLS ON~~  
4 ~~PREVIOUSLY DECONTROLLED PRODUCTS.~~—Any  
5 encryption product not requiring an export license as of  
6 the date of enactment of this Act, as a result of adminis-  
7 trative decision or rulemaking, shall not require an export  
8 license on or after such date of enactment.

9 (c) ~~APPLICABILITY OF CERTAIN EXPORT CON-~~  
10 ~~TROLS.~~—

11 (1) ~~IN GENERAL.~~—Nothing in this Act shall  
12 limit the authority of the President under the Inter-  
13 national Emergency Economic Powers Act, the  
14 Trading with the enemy Act, or the Export Adminis-  
15 tration Act of 1979, to—

16 (A) prohibit the export of encryption prod-  
17 ucts to countries that have been determined to  
18 repeatedly provide support for acts of inter-  
19 national terrorism; or

20 (B) impose an embargo on exports to, and  
21 imports from, a specific country.

22 (2) ~~SPECIFIC DENIALS.~~—The Secretary may  
23 prohibit the export of specific encryption products to  
24 an individual or organization in a specific foreign  
25 country identified by the Secretary, if the Secretary

1 determines that there is substantial evidence that  
2 such encryption products will be used for military or  
3 terrorist end-use.

4 (3) DEFINITION.—As used in this subsection  
5 and subsection (b), the term “encryption” has the  
6 meaning given that term in section 17(g)(5)(A) of  
7 the Export Administration Act of 1979, as added by  
8 subsection (a) of this section.

9 (d) CONTINUATION OF EXPORT ADMINISTRATION  
10 ACT.—For purposes of carrying out the amendment made  
11 by subsection (a), the Export Administration Act of 1979  
12 shall be deemed to be in effect.

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

14 (a) COLLECTION OF INFORMATION BY ATTORNEY  
15 GENERAL.—The Attorney General shall compile, and  
16 maintain in classified form, data on the instances in which  
17 encryption (as defined in section 2801 of title 18, United  
18 States Code) has interfered with, impeded, or obstructed  
19 the ability of the Department of Justice to enforce the  
20 criminal laws of the United States.

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

1 **SECTION 1. SHORT TITLE.**

2 *This Act may be cited as the “Security And Freedom*  
3 *through Encryption (SAFE) Act”.*

4 **SEC. 2. DEFINITIONS.**

5 *For purposes of this Act, the following definitions shall*  
6 *apply:*

7 (1) *COMPUTER HARDWARE.—The term “com-*  
8 *puter hardware” includes computer systems, equip-*  
9 *ment, application-specific assemblies, smart cards,*  
10 *modules, integrated circuits, printed circuit board as-*  
11 *semblies, and devices that incorporate 1 or more*  
12 *microprocessor-based central processing units that are*  
13 *capable of accepting, storing, processing, or providing*  
14 *output of data.*

15 (2) *ENCRYPT AND ENCRYPTION.—The terms*  
16 *“encrypt” and “encryption” means the scrambling*  
17 *(and descrambling) of wire communications, elec-*  
18 *tronic communications, or electronically stored infor-*  
19 *mation, using mathematical formulas or algorithms*  
20 *to preserve the confidentiality, integrity, or authen-*  
21 *ticity of, and prevent unauthorized recipients from*  
22 *accessing or altering, such communications or infor-*  
23 *mation.*

24 (3) *ENCRYPTION PRODUCT.—The term*  
25 *“encryption product”—*

1           (A) means computer hardware, computer  
2 software, or technology with encryption capabili-  
3 ties; and

4           (B) includes any subsequent version of or  
5 update to an encryption product, if the  
6 encryption capabilities are not changed.

7           (4) *KEY*.—The term “key” means the variable  
8 information used in a mathematical formula, code, or  
9 algorithm, or any component thereof, used to decrypt  
10 wire communications, electronic communications, or  
11 electronically stored information, that has been  
12 encrypted.

13           (5) *KEY RECOVERY INFORMATION*.—The term  
14 “key recovery information” means information that  
15 would enable obtaining the key of a user of  
16 encryption.

17           (6) *PERSON*.—The term “person” has the mean-  
18 ing given the term in section 2510 of title 18, United  
19 States Code.

20           (7) *SECRETARY*.—The term “Secretary” means  
21 the Secretary of Commerce.

22           (8) *STATE*.—The term “State” means any State  
23 of the United States and includes the District of Co-  
24 lumbia and any commonwealth, territory, or posses-  
25 sions of the United States.

1           (9) *UNITED STATES PERSON.*—*The term “United*  
2 *States person” means any—*

3                   (A) *United States citizen; or*

4                   (B) *legal entity that—*

5                           (i) *is organized under the laws of the*  
6 *United States, or any States, the District of*  
7 *Columbia, or any commonwealth, territory,*  
8 *or possession of the United States; and*

9                           (ii) *has its principal place of business*  
10 *in the United States.*

11           (10) *WIRE COMMUNICATION; ELECTRONIC COM-*  
12 *MUNICATION.*—*The terms “wire communication” and*  
13 *“electronic communication” have the meanings given*  
14 *such terms in section 2510 of title 18, United States*  
15 *Code.*

16 **SEC. 3. ENSURING DEVELOPMENT AND DEPLOYMENT OF**  
17 **ENCRYPTION IS A VOLUNTARY PRIVATE SEC-**  
18 **TOR ACTIVITY.**

19           (a) *STATEMENT OF POLICY.*—*It is the policy of the*  
20 *United States that the use, development, manufacture, sale,*  
21 *distribution, and importation of encryption products,*  
22 *standards, and services for purposes of assuring the con-*  
23 *fidentiality, authenticity, or integrity of electronic informa-*  
24 *tion shall be voluntary and market driven.*

1           (b) *LIMITATION ON REGULATION.*—Neither the Federal  
2 Government nor a State may establish any conditions, ties,  
3 or links between encryption products, standards, and serv-  
4 ices used for confidentiality, and those used for authenticity  
5 or integrity purposes.

6 **SEC. 4. PROTECTION OF DOMESTIC SALE AND USE OF**  
7                                   **ENCRYPTION.**

8           *Except as otherwise provided by this Act, it is lawful*  
9 *for any person within any State, and for any United States*  
10 *person in a foreign country, to develop, manufacture, sell,*  
11 *distribute, import, or use any encryption product, regard-*  
12 *less of the encryption algorithm selected, encryption key*  
13 *length chosen, existence of key recovery, or other plaintext*  
14 *access capability, or implementation or medium used.*

15 **SEC. 5. PROHIBITION ON MANDATORY GOVERNMENT AC-**  
16                                   **CESS TO PLAINTEXT.**

17           (a) *IN GENERAL.*—No department, agency, or instru-  
18 mentality of the United States or of any State may require  
19 that, set standards for, condition any approval on, create  
20 incentives for, or tie any benefit to a requirement that, a  
21 decryption key, access to a key, key recovery information,  
22 or any other plaintext access capability be—

23                           (1) *required to be built into computer hardware*  
24                           *or software for any purpose;*

1           (2) given to any other person (including a de-  
2           partment, agency, or instrumentality of the United  
3           States or an entity in the private sector that may be  
4           certified or approved by the United States or a  
5           State); or

6           (3) retained by the owner or user of an  
7           encryption key or any other person, other than for  
8           encryption products for the use of the United States  
9           Government or a State government.

10          (b) *PROTECTION OF EXISTING ACCESS.*—Subsection  
11          (a) does not affect the authority of any investigative or law  
12          enforcement officer, or any member of the intelligence com-  
13          munity (as defined in section 3 of the National Security  
14          Act of 1947 (50 U.S.C. 401a)), acting under any law in  
15          effect on the date of the enactment of this Act, to gain access  
16          to encrypted communications or information.

17          **SEC. 6. UNLAWFUL USE OF ENCRYPTION IN FURTHERANCE**  
18                                        **OF A CRIMINAL ACT.**

19          (a) *ENCRYPTION OF INCRIMINATING COMMUNICATIONS*  
20          *OR INFORMATION UNLAWFUL.*—Any person who, in the  
21          commission of a felony under a criminal statute of the  
22          United States, knowingly and willfully encrypts incrimi-  
23          nating communications or information relating to that fel-  
24          ony with the intent to conceal such communications or in-

1 *formation for the purpose of avoiding detection by law en-*  
2 *forcement agencies or prosecution—*

3 *(1) in the case of a first offense under this sec-*  
4 *tion, shall be imprisoned for not more than 5 years,*  
5 *or fined under title 18, United States Code, or both;*  
6 *and*

7 *(2) in the case of a second or subsequent offense*  
8 *under this section, shall be imprisoned for not more*  
9 *than 10 years, or fined under title 18, United States*  
10 *Code, or both.*

11 *(b) USE OF ENCRYPTION NOT A BASIS FOR PROBABLE*  
12 *CAUSE.—The use of encryption by any person shall not be*  
13 *the sole basis for establishing probable cause with respect*  
14 *to a criminal offense or a search warrant.*

15 **SEC. 7. EXPORTS OF ENCRYPTION.**

16 *(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF*  
17 *1979.—Section 17 of the Export Administration Act of*  
18 *1979 (50 U.S.C. App. 2416) is amended by adding at the*  
19 *end the following new subsection:*

20 *“(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS,*  
21 *AND RELATED EQUIPMENT.—*

22 *“(1) GENERAL RULE.—Subject to paragraphs*  
23 *(2), (3), and (4), the Secretary shall have exclusive*  
24 *authority to control exports of all computer hardware,*  
25 *software, computing devices, customer premises equip-*

1 *ment, communications network equipment, and tech-*  
2 *nology for information security (including*  
3 *encryption), except that which is specifically designed*  
4 *or modified for military use, including command,*  
5 *control, and intelligence applications.*

6 “(2) *CRITICAL INFRASTRUCTURE PROTECTION*  
7 *PRODUCTS.—*

8 “(A) *IDENTIFICATION.—Not later than 90*  
9 *days after the date of the enactment of the Secu-*  
10 *rity And Freedom through Encryption (SAFE)*  
11 *Act, the Assistant Secretary of Commerce for*  
12 *Communications and Information and the Na-*  
13 *tional Telecommunications and Information Ad-*  
14 *ministration shall issue regulations that identify,*  
15 *define, or determine which products and equip-*  
16 *ment described in paragraph (1) are designed for*  
17 *improvement of network security, network reli-*  
18 *ability, or data security.*

19 “(B) *NTIA RESPONSIBILITY.—Not later*  
20 *than the expiration of the 2-year period begin-*  
21 *ning on the date of the enactment of the Security*  
22 *And Freedom through Encryption (SAFE) Act,*  
23 *all authority of the Secretary under this sub-*  
24 *section and all determinations and reviews re-*  
25 *quired by this section, with respect to products*

1           *and equipment described in paragraph (1) that*  
2           *are designed for improvement of network secu-*  
3           *rity, network reliability, or data security*  
4           *through the use of encryption, shall be exercised*  
5           *through and made by the Assistant Secretary of*  
6           *Commerce for Communications and Information*  
7           *and the National Telecommunications and Infor-*  
8           *mation Administration. The Secretary may, at*  
9           *any time, assign to the Assistant Secretary and*  
10          *the NTIA authority of the Secretary under this*  
11          *section with respect to other products and equip-*  
12          *ment described in paragraph (1).*

13           “(3) *ITEMS NOT REQUIRING LICENSES.*—*After a*  
14          *one-time technical review by the Secretary of not*  
15          *more than 30 working days, which shall include con-*  
16          *sultation with the Secretary of Defense, the Secretary*  
17          *of State, the Attorney General, and the Director of*  
18          *Central Intelligence, no export license may be re-*  
19          *quired, except pursuant to the Trading with the*  
20          *Enemy Act or the International Emergency Economic*  
21          *Powers Act (but only to the extent that the authority*  
22          *of such Act is not exercised to extend controls imposed*  
23          *under this Act), for the export or reexport of—*

24                   “(A) *any computer hardware or software or*  
25                   *computing device, including computer hardware*

1           *or software or computing devices with encryption*  
2           *capabilities—*

3                     *“(i) that is generally available;*

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

10                    *“(iii) that is used in a commercial, off-*  
11                    *the-shelf, consumer product or any compo-*  
12                    *nent or subassembly designed for use in*  
13                    *such a consumer product available within*  
14                    *the United States or abroad which—*

15                            *“(I) includes encryption capabili-*  
16                            *ties which are inaccessible to the end*  
17                            *user; and*

18                            *“(II) is not designed for military*  
19                            *or intelligence end use;*

20                    *“(B) any computing device solely because it*  
21                    *incorporates or employs in any form—*

22                            *“(i) computer hardware or software*  
23                            *(including computer hardware or software*  
24                            *with encryption capabilities) that is ex-*

1           empted from any requirement for a license  
2           under subparagraph (A); or

3           “(ii) computer hardware or software  
4           that is no more technically complex in its  
5           encryption capabilities than computer hard-  
6           ware or software that is exempted from any  
7           requirement for a license under subpara-  
8           graph (A) but is not designed for installa-  
9           tion by the purchaser;

10          “(C) any computer hardware or software or  
11          computing device solely on the basis that it in-  
12          corporates or employs in any form interface  
13          mechanisms for interaction with other computer  
14          hardware or software or computing devices, in-  
15          cluding computer hardware and software and  
16          computing devices with encryption capabilities;

17          “(D) any computing or telecommunication  
18          device which incorporates or employs in any  
19          form computer hardware or software encryption  
20          capabilities which—

21                 “(i) are not directly available to the  
22                 end user; or

23                 “(ii) limit the encryption to be point-  
24                 to-point from the user to a central commu-

1                    *nications point or link and does not enable*  
2                    *end-to-end user encryption;*

3                    *“(E) technical assistance and technical data*  
4                    *used for the installation or maintenance of com-*  
5                    *puter hardware or software or computing devices*  
6                    *with encryption capabilities covered under this*  
7                    *subsection; or*

8                    *“(F) any encryption hardware or software*  
9                    *or computing device not used for confidentiality*  
10                   *purposes, such as authentication, integrity, elec-*  
11                   *tronic signatures, nonrepudiation, or copy pro-*  
12                   *tection.*

13                   *“(4) COMPUTER HARDWARE OR SOFTWARE OR*  
14                   *COMPUTING DEVICES WITH ENCRYPTION CAPABILI-*  
15                   *TIES.—After a one-time technical review by the Sec-*  
16                   *retary of not more than 30 working days, which shall*  
17                   *include consultation with the Secretary of Defense, the*  
18                   *Secretary of State, the Attorney General, and the Di-*  
19                   *rector of Central Intelligence, the Secretary shall au-*  
20                   *thorize the export or reexport of computer hardware*  
21                   *or software or computing devices with encryption ca-*  
22                   *pabilities for nonmilitary end uses in any country—*

23                   *“(A) to which exports of computer hardware*  
24                   *or software or computing devices of comparable*  
25                   *strength are permitted for use by financial insti-*

1           *tutions not controlled in fact by United States*  
2           *persons, unless there is substantial evidence that*  
3           *such computer hardware or software or com-*  
4           *puting devices will be—*

5                     *“(i) diverted to a military end use or*  
6                     *an end use supporting international ter-*  
7                     *rorism;*

8                     *“(ii) modified for military or terrorist*  
9                     *end use;*

10                    *“(iii) reexported without any author-*  
11                    *ization by the United States that may be*  
12                    *required under this Act; or*

13                    *“(iv)(I) harmful to the national secu-*  
14                    *rity of the United States, including capa-*  
15                    *bilities of the United States in fighting drug*  
16                    *trafficking, terrorism, or espionage, (II)*  
17                    *used in illegal activities involving the sex-*  
18                    *ual exploitation of, abuse of, or sexually ex-*  
19                    *PLICIT conduct with minors (including ac-*  
20                    *tivities in violation of chapter 110 of title*  
21                    *18, United States Code, and section 2423 of*  
22                    *such title), or (III) used in illegal activities*  
23                    *involving organized crime; or*

24                    *“(B) if the Secretary determines that a*  
25                    *computer hardware or software or computing de-*

1           *vice offering comparable security is commercially*  
2           *available in such country from a foreign sup-*  
3           *plier, without effective restrictions.*

4           “(5) *DEFINITIONS.—For purposes of this*  
5           *subsection—*

6                   “(A) *the term ‘computer hardware’ has the*  
7                   *meaning given such term in section 2 of the Se-*  
8                   *curity And Freedom through Encryption*  
9                   *(SAFE) Act;*

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

14                   “(C) *the term ‘customer premises equip-*  
15                   *ment’ means equipment employed on the prem-*  
16                   *ises of a person to originate, route, or terminate*  
17                   *communications;*

18                   “(D) *the term ‘data security’ means the*  
19                   *protection, through techniques used by individual*  
20                   *computer and communications users, of data*  
21                   *from unauthorized penetration, manipulation, or*  
22                   *disclosure;*

23                   “(E) *the term ‘encryption’ has the meaning*  
24                   *given such term in section 2 of the Security And*  
25                   *Freedom through Encryption (SAFE) Act;*

1           “(F) the term ‘generally available’ means,  
2           in the case of computer hardware or computer  
3           software (including computer hardware or com-  
4           puter software with encryption capabilities)—

5                   “(i) computer hardware or computer  
6                   software that is—

7                           “(I) distributed through the Inter-  
8                           net;

9                           “(II) offered for sale, license, or  
10                          transfer to any person without restric-  
11                          tion, whether or not for consideration,  
12                          including, but not limited to, over-the-  
13                          counter retail sales, mail order trans-  
14                          actions, phone order transactions, elec-  
15                          tronic distribution, or sale on ap-  
16                          proval;

17                          “(III) preloaded on computer  
18                          hardware or computing devices that  
19                          are widely available for sale to the  
20                          public; or

21                          “(IV) assembled from computer  
22                          hardware or computer software compo-  
23                          nents that are widely available for sale  
24                          to the public;

1           “(ii) not designed, developed, or tai-  
2           lored by the manufacturer for specific pur-  
3           chasers or users, except that any such pur-  
4           chaser or user may—

5                   “(I) supply certain installation  
6                   parameters needed by the computer  
7                   hardware or software to function prop-  
8                   erly with the computer system of the  
9                   user or purchaser; or

10                   “(II) select from among options  
11                   contained in the computer hardware or  
12                   computer software; and

13           “(iii) with respect to which the manu-  
14           facturer of that computer hardware or com-  
15           puter software—

16                   “(I) intended for the user or pur-  
17                   chaser, including any licensee or trans-  
18                   feree, to install the computer hardware  
19                   or software and has supplied the nec-  
20                   essary instructions to do so, except that  
21                   the manufacturer of the computer  
22                   hardware or software, or any agent of  
23                   such manufacturer, may also provide  
24                   telephone or electronic mail help line

1                    *services for installation, electronic*  
2                    *transmission, or basic operations; and*

3                    *“(II) the computer hardware or*  
4                    *software is designed for such installa-*  
5                    *tion by the user or purchaser without*  
6                    *further substantial support by the*  
7                    *manufacturer;*

8                    *“(G) the term ‘network reliability’ means*  
9                    *the prevention, through techniques used by pro-*  
10                    *viders of computer and communications services,*  
11                    *of the malfunction, and the promotion of the con-*  
12                    *tinued operations, of computer or communica-*  
13                    *tions network;*

14                    *“(H) the term ‘network security’ means the*  
15                    *prevention, through techniques used by providers*  
16                    *of computer and communications services, of un-*  
17                    *authorized penetration, manipulation, or disclo-*  
18                    *sure of information of a computer or commu-*  
19                    *nications network;*

20                    *“(I) the term ‘technical assistance’ includes*  
21                    *instruction, skills training, working knowledge,*  
22                    *consulting services, and the transfer of technical*  
23                    *data;*

24                    *“(J) the term ‘technical data’ includes blue-*  
25                    *prints, plans, diagrams, models, formulas, tables,*

1           *engineering designs and specifications, and*  
2           *manuals and instructions written or recorded on*  
3           *other media or devices such as disks, tapes, or*  
4           *read-only memories; and*

5                   “(K) the term ‘technical review’ means a re-  
6           *view by the Secretary of computer hardware or*  
7           *software or computing devices with encryption*  
8           *capabilities, based on information about the*  
9           *product’s encryption capabilities supplied by the*  
10          *manufacturer, that the computer hardware or*  
11          *software or computing device works as rep-*  
12          *resented.”.*

13          (b) *TRANSFER OF AUTHORITY TO NATIONAL TELE-*  
14          *COMMUNICATIONS AND INFORMATION ADMINISTRATION.—*  
15          *Section 103(b) of the National Telecommunications and In-*  
16          *formation Administration Organization Act (47 U.S.C.*  
17          *902(b)) is amended by adding at the end the following new*  
18          *paragraph:*

19                   “(4) *EXPORT OF COMMUNICATIONS TRANSACTION*  
20          *TECHNOLOGIES.—In accordance with section 17(g)(2)*  
21          *of the Export Administration Act of 1979 (50 U.S.C.*  
22          *App. 2416(g)(2)), the Secretary shall assign to the As-*  
23          *stant Secretary and the NTIA the authority of the*  
24          *Secretary under such section 17(g), with respect to*  
25          *products and equipment described in paragraph (1)*

1       of such section that are designed for improvement of  
2       network security, network reliability, or data security,  
3       that (after the expiration of the 2-year period begin-  
4       ning on the date of the enactment of the Security And  
5       Freedom through Encryption (SAFE) Act) is to be  
6       exercised by the Assistant Secretary and the NTIA.”.

7       (c) *NO REINSTATEMENT OF EXPORT CONTROLS ON*  
8       *PREVIOUSLY DECONTROLLED PRODUCTS.*—Any encryption  
9       product not requiring an export license as of the date of  
10      enactment of this Act, as a result of administrative decision  
11      or rulemaking, shall not require an export license on or  
12      after such date of enactment.

13      (d) *APPLICABILITY OF CERTAIN EXPORT CONTROLS.*—

14           (1) *IN GENERAL.*—Nothing in this Act shall  
15      limit the authority of the President under the Inter-  
16      national Emergency Economic Powers Act, the Trad-  
17      ing with the Enemy Act, or the Export Administra-  
18      tion Act of 1979, to—

19           (A) prohibit the export of encryption prod-  
20      ucts to countries that have been determined to re-  
21      peatedly provide support for acts of inter-  
22      national terrorism; or

23           (B) impose an embargo on exports to, and  
24      imports from, a specific country.

1           (2) *SPECIFIC DENIALS.*—*The Secretary of Com-*  
2           *merce may prohibit the export of specific encryption*  
3           *products to an individual or organization in a spe-*  
4           *cific foreign country identified by the Secretary, if the*  
5           *Secretary determines that there is substantial evi-*  
6           *dence that such encryption products will be—*

7                     (A) *used for military or terrorist end-use or*  
8                     *modified for military or terrorist end use;*

9                     (B) *harmful to United States national secu-*  
10                    *urity, including United States capabilities in*  
11                    *fighting drug trafficking, terrorism, or espionage;*

12                    (C) *used in illegal activities involving the*  
13                    *sexual exploitation of, abuse of, or sexually ex-*  
14                    *PLICIT conduct with minors (including activities*  
15                    *in violation of chapter 110 of title 18, United*  
16                    *States Code, and section 2423 of such title); or*

17                    (D) *used in illegal activities involving orga-*  
18                    *nized crime.*

19           (3) *OTHER EXPORT CONTROLS.*—*An encryption*  
20           *product is subject to any export control imposed on*  
21           *that product for any reason other than the existence*  
22           *of encryption capability. Nothing in this Act or the*  
23           *amendments made by this Act alters the ability of the*  
24           *Secretary of Commerce to control exports of products*  
25           *for reasons other than encryption.*

1       (e) *CONTINUATION OF EXPORT ADMINISTRATION*  
2 *ACT.*—*For purposes of carrying out the amendment made*  
3 *by subsection (a), the Export Administration Act of 1979*  
4 *shall be deemed to be in effect.*

5 **SEC. 8. GOVERNMENT PROCUREMENT OF ENCRYPTION**  
6 **PRODUCTS.**

7       (a) *STATEMENT OF POLICY.*—*It is the policy of the*  
8 *United States—*

9               (1) *to permit the public to interact with govern-*  
10 *ment through commercial networks and infrastruc-*  
11 *ture; and*

12               (2) *to protect the privacy and security of any*  
13 *electronic communication from, or stored information*  
14 *obtained from, the public.*

15       (b) *PURCHASE OF ENCRYPTION PRODUCTS BY FED-*  
16 *ERAL GOVERNMENT.*—*Any department, agency, or instru-*  
17 *mentality of the United States may purchase encryption*  
18 *products for internal use by officers and employees of the*  
19 *United States to the extent and in the manner authorized*  
20 *by law.*

21       (c) *PROHIBITION OF REQUIREMENT FOR CITIZENS TO*  
22 *PURCHASE SPECIFIED PRODUCTS.*—*No department, agen-*  
23 *cy, or instrumentality of the United States, nor any depart-*  
24 *ment, agency, or political subdivision of a State, may re-*  
25 *quire any person in the private sector to use any particular*

1 *encryption product or methodology, including products*  
 2 *with a decryption key, access to a key, key recovery infor-*  
 3 *mation, or any other plaintext access capability, to commu-*  
 4 *nicate with, or transact business with, the government.*

5 **SEC. 9. NATIONAL ELECTRONIC TECHNOLOGIES CENTER.**

6 *Part A of the National Telecommunications and Infor-*  
 7 *mation Administration Organization Act is amended by*  
 8 *inserting after section 105 (47 U.S.C. 904) the following*  
 9 *new section:*

10 **“SEC. 106. NATIONAL ELECTRONIC TECHNOLOGIES CEN-**  
 11 **TER.**

12 *“(a) ESTABLISHMENT.—There is established in the*  
 13 *NTIA a National Electronic Technologies Center (in this*  
 14 *section referred to as the ‘NET Center’).*

15 *“(b) DIRECTOR.—The NET Center shall have a Direc-*  
 16 *tor, who shall be appointed by the Assistant Secretary.*

17 *“(c) DUTIES.—The duties of the NET Center shall*  
 18 *be—*

19 *“(1) to serve as a center for industry and govern-*  
 20 *ment entities to exchange information and method-*  
 21 *ology regarding data security techniques and tech-*  
 22 *nologies;*

23 *“(2) to examine encryption techniques and meth-*  
 24 *ods to facilitate the ability of law enforcement to gain*

1 *efficient access to plaintext of communications and*  
2 *electronic information;*

3 *“(3) to conduct research to develop efficient*  
4 *methods, and improve the efficiency of existing meth-*  
5 *ods, of accessing plaintext of communications and*  
6 *electronic information;*

7 *“(4) to investigate and research new and emerg-*  
8 *ing techniques and technologies to facilitate access to*  
9 *communications and electronic information, includ-*  
10 *ing —*

11 *“(A) reverse-steganography;*

12 *“(B) decompression of information that pre-*  
13 *viously has been compressed for transmission;*  
14 *and*

15 *“(C) de-multiplexing;*

16 *“(5) to obtain information regarding the most*  
17 *current computer hardware and software, tele-*  
18 *communications, and other capabilities to understand*  
19 *how to access information transmitted across com-*  
20 *puter and communications networks; and*

21 *“(6) to serve as a center for Federal, State, and*  
22 *local law enforcement authorities for information and*  
23 *assistance regarding decryption and other access re-*  
24 *quirements.*

1       “(d) *EQUAL ACCESS.*—*State and local law enforce-*  
2 *ment agencies and authorities shall have access to informa-*  
3 *tion, services, resources, and assistance provided by the*  
4 *NET Center to the same extent that Federal law enforce-*  
5 *ment agencies and authorities have such access.*

6       “(e) *PERSONNEL.*—*The Director may appoint such*  
7 *personnel as the Director considers appropriate to carry out*  
8 *the duties of the NET Center.*

9       “(f) *ASSISTANCE OF OTHER FEDERAL AGENCIES.*—  
10 *Upon the request of the Director of the NET Center, the*  
11 *head of any department or agency of the Federal Govern-*  
12 *ment may, to assist the NET Center in carrying out its*  
13 *duties under this section—*

14               “(1) *detail, on a reimbursable basis, any of the*  
15 *personnel of such department or agency to the NET*  
16 *Center; and*

17               “(2) *provide to the NET Center facilities, infor-*  
18 *mation, and other non-personnel resources.*

19       “(g) *PRIVATE INDUSTRY ASSISTANCE.*—*The NET Cen-*  
20 *ter may accept, use, and dispose of gifts, bequests, or devises*  
21 *of money, services, or property, both real and personal, for*  
22 *the purpose of aiding or facilitating the work of the Center.*  
23 *Gifts, bequests, or devises of money and proceeds from sales*  
24 *of other property received as gifts, bequests, or devises shall*

1 *be deposited in the Treasury and shall be available for dis-*  
2 *bursement upon order of the Director of the NET Center.*

3 “(h) *ADVISORY BOARD.*—

4 “(1) *ESTABLISHMENT.*—*There is established the*  
5 *Advisory Board of the NET Center (in this subsection*  
6 *referred to as the “Advisory Board”), which shall be*  
7 *comprised of 11 members who shall have the quali-*  
8 *fications described in paragraph (2) and who shall be*  
9 *appointed by the Assistant Secretary not later than*  
10 *6 months after the date of the enactment of this Act.*  
11 *The chairman of the Advisory Board shall be des-*  
12 *ignated by the Assistant Secretary at the time of ap-*  
13 *pointment.*

14 “(2) *QUALIFICATIONS.*—*Each member of the Ad-*  
15 *visory Board shall have experience or expertise in the*  
16 *field of encryption, decryption, electronic communica-*  
17 *tion, information security, electronic commerce, or*  
18 *law enforcement.*

19 “(3) *DUTIES.*—*The duty of the Advisory Board*  
20 *shall be to advise the NET Center and the Federal*  
21 *Government regarding new and emerging technologies*  
22 *relating to encryption and decryption of communica-*  
23 *tions and electronic information.*

24 “(i) *IMPLEMENTATION PLAN.*—*Within 2 months after*  
25 *the date of the enactment of this Act, the Assistant Sec-*

1 *retary, in consultation and cooperation with other appro-*  
2 *priate Federal agencies and appropriate industry partici-*  
3 *pants, develop and cause to be published in the Federal Reg-*  
4 *ister a plan for establishing the NET Center. The plan*  
5 *shall—*

6           “(1) *specify the physical location of the NET*  
7 *Center and the equipment, software, and personnel re-*  
8 *sources necessary to carry out the duties of the NET*  
9 *Center under this section;*

10           “(2) *assess the amount of funding necessary to*  
11 *establish and operate the NET Center; and*

12           “(3) *identify sources of probable funding for the*  
13 *NET Center, including any sources of in-kind con-*  
14 *tributions from private industry.”.*

15 **SEC. 10. STUDY OF NETWORK AND DATA SECURITY ISSUES.**

16       *Part C of the National Telecommunications and Infor-*  
17 *mation Administration Organization Act is amended by*  
18 *adding at the end the following new section:*

19 **“SEC. 156. STUDY OF NETWORK RELIABILITY AND SECURITY**  
20 **AND DATA SECURITY ISSUES.**

21       “(a) *IN GENERAL.—The NTIA shall conduct an exam-*  
22 *ination of—*

23           “(1) *the relationship between—*

24               “(A) *network reliability (for communica-*  
25 *tions and computer networks), network security*

1           *(for such networks), and data security issues;*  
2           *and*

3           *“(B) the conduct, in interstate commerce, of*  
4           *electronic commerce transactions, including*  
5           *through the medium of the telecommunications*  
6           *networks, the Internet, or other interactive com-*  
7           *puter systems;*

8           *“(2) the availability of various methods for*  
9           *encrypting communications; and*

10           *“(3) the effects of various methods of providing*  
11           *access to encrypted communications and to informa-*  
12           *tion to further law enforcement activities.*

13           *“(b) SPECIFIC ISSUES.—In conducting the examina-*  
14           *tion required by subsection (a), the NTIA shall—*

15           *“(1) analyze and evaluate the requirements*  
16           *under paragraphs (3) and (4) of section 17(g) of the*  
17           *Export Administration Act of 1979 (50 U.S.C. App.*  
18           *2416(g); as added by section 7(a) of this Act) for*  
19           *products referred to in such paragraphs to qualify for*  
20           *the license exemption or mandatory export authoriza-*  
21           *tion under such paragraphs, and determine—*

22           *“(A) the scope and applicability of such re-*  
23           *quirements and the products that, at the time of*  
24           *the examination, qualify for such license exemp-*  
25           *tion or export authorization; and*

1           “(B) the products that will, 12 months after  
2           the examination is conducted, qualify for such li-  
3           cense exemption or export authorization; and

4           “(2) assess possible methods for providing access  
5           to encrypted communications and to information to  
6           further law enforcement activities.

7           “(c) *REPORTS.*—Within one year after the date of en-  
8           actment of this section, the NTIA shall submit to the Con-  
9           gress and the President a detailed report on the examina-  
10          tion required by subsections (a) and (b). Annually there-  
11          after, the NTIA shall submit to the Congress and the Presi-  
12          dent an update on such report.

13          “(d) *DEFINITIONS.*—For purposes of this section—

14                 “(1) the terms ‘data security’, ‘encryption’, ‘net-  
15                 work reliability’, and ‘network security’ have the  
16                 meanings given such terms in section 17(g)(5) of the  
17                 Export Administration Act of 1979 (50 U.S.C. App.  
18                 2416(g)(5)); and

19                 “(2) the terms ‘Internet’ and ‘interactive com-  
20                 puter systems’ have the meanings provided by section  
21                 230(e) of the Communications Act of 1934 (47 U.S.C.  
22                 230(e)).”.

1 **SEC. 11. TREATMENT OF ENCRYPTION IN INTERSTATE AND**  
2 **FOREIGN COMMERCE.**

3 (a) *INQUIRY REGARDING IMPEDIMENTS TO COM-*  
4 *MERCE.*—*Within 180 days after the date of the enactment*  
5 *of this Act, the Secretary of Commerce shall complete an*  
6 *inquiry to—*

7 (1) *identify any domestic and foreign impedi-*  
8 *ments to trade in encryption products and services*  
9 *and the manners in which and extent to which such*  
10 *impediments inhibit the development of interstate and*  
11 *foreign commerce; and*

12 (2) *identify import restrictions imposed by for-*  
13 *ign nations that constitute trade barriers to pro-*  
14 *viders of encryption products or services.*

15 *The Secretary shall submit a report to the Congress regard-*  
16 *ing the results of such inquiry by such date.*

17 (b) *REMOVAL OF IMPEDIMENTS TO TRADE.*—*Within 1*  
18 *year after such date of enactment, the Secretary shall pre-*  
19 *scribe such regulations as may be necessary to reduce the*  
20 *impediments to trade in encryption products and services*  
21 *identified in the inquiry pursuant to subsection (a) for the*  
22 *purpose of facilitating the development of interstate and for-*  
23 *ign commerce. Such regulations shall be designed to—*

24 (1) *promote the sale and distribution, including*  
25 *through electronic commerce, in foreign commerce of*

1 *encryption products and services manufactured in the*  
2 *United States; and*

3 *(2) strengthen the competitiveness of domestic*  
4 *providers of encryption products and services in for-*  
5 *foreign commerce, including electronic commerce.*

6 *(c) INTERNATIONAL AGREEMENTS.—*

7 *(1) REPORT TO PRESIDENT.—Upon the comple-*  
8 *tion of the inquiry under subsection (a), the Secretary*  
9 *shall submit a report to the President regarding re-*  
10 *ducing any impediments to trade in encryption prod-*  
11 *ucts and services that are identified by the inquiry*  
12 *and could, in the determination of the Secretary, re-*  
13 *quire international negotiations for such reduction.*

14 *(2) NEGOTIATIONS.—The President shall take all*  
15 *actions necessary to conduct negotiations with other*  
16 *countries for the purposes of (A) concluding inter-*  
17 *national agreements on the promotion of encryption*  
18 *products and services, and (B) achieving mutual rec-*  
19 *ognition of countries' export controls, in order to meet*  
20 *the needs of countries to preserve national security,*  
21 *safeguard privacy, and prevent commercial espionage.*  
22 *The President may consider a country's refusal to ne-*  
23 *gotiate such international export and mutual recogni-*  
24 *tion agreements when considering the participation of*  
25 *the United States in any cooperation or assistance*

1        *program with that country. The President shall sub-*  
 2        *mit a report to the Congress regarding the status of*  
 3        *international efforts regarding cryptography not later*  
 4        *than December 31, 2000.*

5    **SEC. 12. COLLECTION OF INFORMATION ON EFFECT OF**  
 6                            **ENCRYPTION ON LAW ENFORCEMENT ACTIVI-**  
 7                            **TIES.**

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

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

19    **SEC. 13. PROHIBITION ON TRANSFERS TO PLA AND COM-**  
 20                            **MUNIST CHINESE MILITARY COMPANIES.**

21        *(a) PROHIBITION.—Whoever knowingly and willfully*  
 22        *transfers to the People’s Liberation Army or to any Com-*  
 23        *munist Chinese military company any encryption product*  
 24        *that utilizes a key length of more than 56 bits—*

1           (1) *in the case of a first offense under this sec-*  
2 *tion, shall be imprisoned for not more than 5 years,*  
3 *or fined under title 18, United States Code, or both;*  
4 *and*

5           (2) *in the case of second or subsequent offense*  
6 *under this section, shall be imprisoned for not more*  
7 *than 10 years, or fined under title 18, United States*  
8 *Code, or both.*

9           (b) *DEFINITIONS.—For purposes of this section:*

10           (1) *COMMUNIST CHINESE MILITARY COMPANY.—*

11           (A) *Subject to subparagraph (B), the term “Com-*  
12 *munist Chinese military company” has the meaning*  
13 *given that term in section 1237(b)(4) of the Strom*  
14 *Thurmond National Defense Authorization Act for*  
15 *Fiscal Year 1999 (50 U.S.C. 1701 note).*

16           (B) *At such time as the determination and pub-*  
17 *lication of persons are made under section 1237(b)(1)*  
18 *of the Strom Thurmond National Defense Authoriza-*  
19 *tion Act for Fiscal Year 1999, the term “Communist*  
20 *Chinese military company” shall mean the list of*  
21 *those persons so published, as revised under section*  
22 *1237(b)(2) of that Act.*

23           (2) *PEOPLE’S LIBERATION ARMY.—The term*  
24 *“People’s Liberation Army” has the meaning given*  
25 *that term in section 1237(c) of the Strom Thurmond*

1       *National Defense Authorization Act for Fiscal Year*  
2       *1999.*

3       **SEC. 14. FAILURE TO DECRYPT INFORMATION OBTAINED**  
4                           **UNDER COURT ORDER.**

5       *Whoever is required by an order of any court to pro-*  
6       *vide to the court or any other party any information in*  
7       *such person's possession which has been encrypted and who,*  
8       *having possession of the key or such other capability to*  
9       *decrypt such information into the readable or comprehen-*  
10      *sible format of such information prior to its encryption,*  
11      *fails to provide such information in accordance with the*  
12      *order in such readable or comprehensible form—*

13               *(1) in the case of a first offense under this sec-*  
14      *tion, shall be imprisoned for not more than 5 years,*  
15      *or fined under title 18, United States Code, or both;*  
16      *and*

17               *(2) in the case of second or subsequent offense*  
18      *under this section, shall be imprisoned for not more*  
19      *than 10 years, or fined under title 18 United States*  
20      *Code, or both.*

21      **SECTION 1. SHORT TITLE.**

22               **This Act may be cited as the “Security**  
23      **And Freedom through Encryption (SAFE)**  
24      **Act”.**

1 SEC. 2. SALE AND USE OF ENCRYPTION.

2 (a) IN GENERAL.—Part I of title 18, United  
3 States Code, is amended by inserting after  
4 chapter 123 the following new chapter:

5 “CHAPTER 125—ENCRYPTED WIRE AND  
6 ELECTRONIC INFORMATION

“Sec.

“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.

7 “§ 2801. Definitions

8 “As used in this chapter—

9 “(1) the terms ‘person’, ‘State’, ‘wire  
10 communication’, ‘electronic communica-  
11 tion’, ‘investigative or law enforcement  
12 officer’, and ‘judge of competent jurisdic-  
13 tion’ have the meanings given those  
14 terms in section 2510 of this title;

15 “(2) the term ‘decrypt’ means to re-  
16 transform or unscramble encrypted data,  
17 including communications, to its read-  
18 able form;

19 “(3) the terms ‘encrypt’, ‘encrypted’,  
20 and ‘encryption’ mean the scrambling of  
21 wire communications, electronic commu-  
22 nications, or electronically stored infor-

1        **mation, using mathematical formulas or**  
2        **algorithms in order to preserve the con-**  
3        **fidentiality, integrity, or authenticity of,**  
4        **and prevent unauthorized recipients**  
5        **from accessing or altering, such commu-**  
6        **nications or information;**

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

14           **“(5) the term ‘key recovery informa-**  
15       **tion’ means information that would en-**  
16       **able obtaining the key of a user of**  
17       **encryption;**

18           **“(6) the term ‘plaintext access capa-**  
19       **bility’ means any method or mechanism**  
20       **which would provide information in**  
21       **readable form prior to its being**  
22       **encrypted or after it has been decrypted;**

23           **“(7) the term ‘United States person’**  
24       **means—**

25            **“(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) GENERAL PROHIBITION.—Neither the**  
3 **Federal Government nor a State may require**  
4 **that, or condition any approval on a require-**  
5 **ment that, a key, access to a key, key recovery**  
6 **information, or any other plaintext access ca-**  
7 **pability be—**

8 **“(1) built into computer hardware or**  
9 **software for any purpose;**

10 **“(2) given to any other person, includ-**  
11 **ing a Federal Government agency or an**  
12 **entity in the private sector that may be**  
13 **certified or approved by the Federal Gov-**  
14 **ernment or a State to receive it; or**

15 **“(3) retained by the owner or user of**  
16 **an encryption key or any other person,**  
17 **other than for encryption products for**  
18 **use by the Federal Government or a**  
19 **State.**

20 **“(b) EXCEPTION FOR GOVERNMENT NATIONAL**  
21 **SECURITY AND LAW ENFORCEMENT PURPOSES.—**  
22 **The prohibition contained in subsection (a)**  
23 **shall not apply to any department, agency, or**  
24 **instrumentality of the United States, or to any**  
25 **department, agency, or political subdivision**  
26 **of a State, that has a valid contract with a**

1 nongovernmental entity that is assisting in  
2 the performance of national security or law  
3 enforcement activity.

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

14 “§ 2805. Unlawful use of encryption in furtherance of  
15                           a criminal act

16       “(a) ENCRYPTION OF INCRIMINATING COMMU-  
17 NICATIONS OR INFORMATION UNLAWFUL.—Any  
18 person who, in the commission of a felony  
19 under a criminal statute of the United States,  
20 knowingly and willfully encrypts incrimi-  
21 nating communications or information relat-  
22 ing to that felony with the intent to conceal  
23 such communications or information for the  
24 purpose of avoiding detection by law enforce-  
25 ment agencies or prosecution—

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

5           “(2) in the case of a second or subse-  
6           quent offense under this section, shall be  
7           imprisoned for not more than 10 years, or  
8           fined in the amount set forth in this title,  
9           or both.

10          “(b) USE OF ENCRYPTION NOT A BASIS FOR  
11          PROBABLE CAUSE.—The use of encryption by  
12          any person shall not be the sole basis for es-  
13          tablishing probable cause with respect to a  
14          criminal offense or a search warrant.”.

15          (b) CONFORMING AMENDMENT.—The table of  
16          chapters for part I of title 18, United States  
17          Code, is amended by inserting after the item  
18          relating to chapter 123 the following new  
19          item:

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

20          SEC. 3. EXPORTS OF ENCRYPTION.

21          (a) AMENDMENT TO EXPORT ADMINISTRATION  
22          ACT OF 1979.—Section 17 of the Export Admin-  
23          istration Act of 1979 (50 U.S.C. App. 2416) is  
24          amended by adding at the end thereof the fol-  
25          lowing new subsection:

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

3           **“(1) GENERAL RULE.—Subject to para-**  
4 **graphs (2) and (3), the Secretary shall**  
5 **have exclusive authority to control ex-**  
6 **ports of all computer hardware, software,**  
7 **computing devices, customer premises**  
8 **equipment, communications network**  
9 **equipment, and technology for informa-**  
10 **tion security (including encryption), ex-**  
11 **cept that which is specifically designed**  
12 **or modified for military use, including**  
13 **command, control, and intelligence appli-**  
14 **cations.**

15           **“(2) ITEMS NOT REQUIRING LICENSES.—**  
16 **After a 1-time technical review by the**  
17 **Secretary, which shall be completed not**  
18 **later than 30 working days after submis-**  
19 **sion of the product concerned for such**  
20 **technical review, no export license may**  
21 **be required, except pursuant to the Trad-**  
22 **ing with the enemy Act or the Inter-**  
23 **national Emergency Economic Powers**  
24 **Act (but only to the extent that the au-**  
25 **thority of such Act is not exercised to ex-**

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

3               **“(A) any computer hardware or**  
4               **software or computing device, includ-**  
5               **ing computer hardware or software**  
6               **or computing devices with encryption**  
7               **capabilities—**

8                       **“(i) that is generally available;**

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

17                      **“(iii) that is used in a commer-**  
18                      **cial, off-the-shelf, consumer prod-**  
19                      **uct or any component or sub-**  
20                      **assembly designed for use in such**  
21                      **a consumer product available**  
22                      **within the United States or**  
23                      **abroad which—**

1           “(I) includes encryption  
2           capabilities which are inac-  
3           cessible to the end user; and

4           “(II) is not designed for  
5           military or intelligence end  
6           use;

7           “(B) any computing device solely  
8           because it incorporates or employs in  
9           any form—

10           “(i) computer hardware or  
11           software (including computer  
12           hardware or software with  
13           encryption capabilities) that is  
14           exempted from any requirement  
15           for a license under subparagraph  
16           (A); or

17           “(ii) computer hardware or  
18           software that is no more tech-  
19           nically complex in its encryption  
20           capabilities than computer hard-  
21           ware or software that is exempted  
22           from any requirement for a li-  
23           cense under subparagraph (A) but  
24           is not designed for installation by  
25           the purchaser;

1           **“(C) any computer hardware or**  
2 **software or computing device solely**  
3 **on the basis that it incorporates or**  
4 **employs in any form interface mecha-**  
5 **nisms for interaction with other com-**  
6 **puter hardware or software or com-**  
7 **puting devices, including computer**  
8 **hardware and software and com-**  
9 **puting devices with encryption capa-**  
10 **bilities;**

11           **“(D) any computing or tele-**  
12 **communication device which incor-**  
13 **porates or employs in any form com-**  
14 **puter hardware or software**  
15 **encryption capabilities which—**

16                   **“(i) are not directly available**  
17 **to the end user; or**

18                   **“(ii) limit the encryption to be**  
19 **point-to-point from the user to a**  
20 **central communications point or**  
21 **link and does not enable end-to-**  
22 **end user encryption;**

23           **“(E) technical assistance and**  
24 **technical data used for the installa-**  
25 **tion or maintenance of computer**

1 hardware or software or computing  
2 devices with encryption capabilities  
3 covered under this subsection; or

4 “(F) any encryption hardware or  
5 software or computing device not  
6 used for confidentiality purposes,  
7 such as authentication, integrity,  
8 electronic signatures, nonrepudi-  
9 ation, or copy protection.

10 “(3) COMPUTER HARDWARE OR SOFT-  
11 WARE OR COMPUTING DEVICES WITH  
12 ENCRYPTION CAPABILITIES.—After a 1-time  
13 technical review by the Secretary, which  
14 shall be completed not later than 30  
15 working days after submission of the  
16 product concerned for such technical re-  
17 view, the Secretary shall authorize the  
18 export or reexport of computer hardware  
19 or software or computing devices with  
20 encryption capabilities for nonmilitary  
21 end uses in any country—

22 “(A) to which exports of computer  
23 hardware or software or computing  
24 devices of comparable strength are  
25 permitted for use by financial institu-

1           **tions not controlled in fact by United**  
2           **States persons, unless there is cred-**  
3           **ible evidence that such computer**  
4           **hardware or software or computing**  
5           **devices will be—**

6                   **“(i) diverted to a military end**  
7                   **use or an end use supporting**  
8                   **international terrorism;**

9                   **“(ii) modified for military or**  
10                   **terrorist end use; or**

11                   **“(iii) reexported without any**  
12                   **authorization by the United**  
13                   **States that may be required**  
14                   **under this Act; or**

15                   **“(B) if the Secretary determines**  
16                   **that a computer hardware or soft-**  
17                   **ware or computing device offering**  
18                   **comparable security is commercially**  
19                   **available outside the United States**  
20                   **from a foreign supplier, without ef-**  
21                   **fective restrictions.**

22                   **“(4) EXPORTS TO MAJOR DRUG-TRANSIT**  
23                   **AND ILLICIT DRUG PRODUCING COUNTRIES.—**  
24                   **The Secretary, before approving any ex-**  
25                   **port or reexport of encryption products**

1 to any major drug-transit country or  
2 major illicit drug producing country  
3 identified under section 490(h) of the For-  
4 eign Assistance Act of 1961, shall consult  
5 with the Attorney General of the United  
6 States, the Director of the Federal Bu-  
7 reau of Investigation, and the Adminis-  
8 trator of the Drug Enforcement Adminis-  
9 tration on the potential impact of such  
10 export or reexport on the flow of illicit  
11 drugs into the United States. This para-  
12 graph shall not authorize the denial of an  
13 export of an encryption product, or of the  
14 issuance of a specific export license, for  
15 which such denial is not otherwise appro-  
16 priate, solely because the country of des-  
17 tination is a major drug-transit country  
18 or major illicit drug producing country.

19 “(5) DEFINITIONS.—As used in this  
20 subsection—

21 “(A)(i) the term ‘encryption’  
22 means the scrambling of wire commu-  
23 nications, electronic communications,  
24 or electronically stored information,  
25 using mathematical formulas or algo-

1           rithms in order to preserve the con-  
2           fidentiality, integrity, or authenticity  
3           of, and prevent unauthorized recipi-  
4           ents from accessing or altering, such  
5           communications or information;

6           “(ii) the terms ‘wire communica-  
7           tion’ and ‘electronic communication’  
8           have the meanings given those terms  
9           in section 2510 of title 18, United  
10          States Code;

11          “(B) the term ‘generally available’  
12          means, in the case of computer hard-  
13          ware or computer software (including  
14          computer hardware or computer soft-  
15          ware with encryption capabilities)—

16                  “(i) computer hardware or  
17                  computer software that is—

18                          “(I) distributed through  
19                          the Internet;

20                          “(II) offered for sale, li-  
21                          cense, or transfer to any per-  
22                          son without restriction,  
23                          whether or not for consider-  
24                          ation, including, but not lim-  
25                          ited to, over-the-counter retail

1 sales, mail order transactions,  
2 phone order transactions,  
3 electronic distribution, or sale  
4 on approval;

5 “(III) preloaded on com-  
6 puter hardware or computing  
7 devices that are widely avail-  
8 able for sale to the public; or

9 “(IV) assembled from com-  
10 puter hardware or computer  
11 software components that are  
12 widely available for sale to  
13 the public;

14 “(ii) not designed, developed,  
15 or tailored by the manufacturer  
16 for specific purchasers or users,  
17 except that any such purchaser or  
18 user may—

19 “(I) supply certain instal-  
20 lation parameters needed by  
21 the computer hardware or  
22 software to function properly  
23 with the computer system of  
24 the user or purchaser; or

1           **“(II) select from among**  
2           **options contained in the com-**  
3           **puter hardware or computer**  
4           **software;**

5           **“(iii) with respect to which**  
6           **the manufacturer of that com-**  
7           **puter hardware or computer**  
8           **software—**

9           **“(I) intended for the user**  
10           **or purchaser, including any li-**  
11           **icensee or transferee, to install**  
12           **the computer hardware or**  
13           **software and has supplied the**  
14           **necessary instructions to do**  
15           **so, except that the manufac-**  
16           **turer of the computer hard-**  
17           **ware or software, or any**  
18           **agent of such manufacturer,**  
19           **may also provide telephone or**  
20           **electronic mail help line serv-**  
21           **ices for installation, elec-**  
22           **tronic transmission, or basic**  
23           **operations; and**

24           **“(II) the computer hard-**  
25           **ware or software is designed**

1           **for such installation by the**  
2           **user or purchaser without**  
3           **further substantial support by**  
4           **the manufacturer; and**

5           **“(iv) offered for sale, license,**  
6           **or transfer to any person without**  
7           **restriction, whether or not for**  
8           **consideration, including, but not**  
9           **limited to, over-the-counter retail**  
10          **sales, mail order transactions,**  
11          **phone order transactions, elec-**  
12          **tronic distribution, or sale on ap-**  
13          **proval;**

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

20          **“(D) the term ‘computer hard-**  
21          **ware’ includes, but is not limited to,**  
22          **computer systems, equipment, appli-**  
23          **cation-specific assemblies, smart**  
24          **cards, modules, integrated circuits,**  
25          **and printed circuit board assemblies;**

1           **“(E) the term ‘customer premises**  
2 **equipment’ means equipment em-**  
3 **ployed on the premises of a person to**  
4 **originate, route, or terminate commu-**  
5 **nications;**

6           **“(F) the term ‘technical assist-**  
7 **ance’ includes instruction, skills**  
8 **training, working knowledge, con-**  
9 **sulting services, and the transfer of**  
10 **technical data;**

11           **“(G) the term ‘technical data’ in-**  
12 **cludes blueprints, plans, diagrams,**  
13 **models, formulas, tables, engineering**  
14 **designs and specifications, and manu-**  
15 **als and instructions written or re-**  
16 **corded on other media or devices**  
17 **such as disks, tapes, or read-only**  
18 **memories; and**

19           **“(H) the term ‘technical review’**  
20 **means a review by the Secretary of**  
21 **computer hardware or software or**  
22 **computing devices with encryption**  
23 **capabilities, based on information**  
24 **about the product’s encryption capa-**  
25 **bilities supplied by the manufacturer,**

1           that the computer hardware or soft-  
2           ware or computing device works as  
3           represented.”.

4           **(b) NO REINSTATEMENT OF EXPORT CON-**  
5 **TROLS ON PREVIOUSLY DECONTROLLED PROD-**  
6 **UCTS.—Any encryption product not requiring**  
7 **an export license as of the date of enactment**  
8 **of this Act, as a result of administrative deci-**  
9 **sion or rulemaking, shall not require an ex-**  
10 **port license on or after such date of enact-**  
11 **ment.**

12           **(c) APPLICABILITY OF CERTAIN EXPORT CON-**  
13 **TROLS.—**

14           **(1) IN GENERAL.—Nothing in this Act**  
15 **shall limit the authority of the President**  
16 **under the International Emergency Eco-**  
17 **nomic Powers Act, the Trading with the**  
18 **enemy Act, or the Export Administration**  
19 **Act of 1979, to—**

20                   **(A) prohibit the export of**  
21 **encryption products to countries that**  
22 **have been determined to repeatedly**  
23 **provide support for acts of inter-**  
24 **national terrorism;**

1           **(B) prohibit the export or reex-**  
2           **port of any encryption product with**  
3           **an encryption strength of more than**  
4           **56 bits to any military unit of the**  
5           **People’s Republic of China, including**  
6           **the People’s Liberation Army (as de-**  
7           **defined in section 1237(c) of the Strom**  
8           **Thurmond National Defense Author-**  
9           **ization Act for Fiscal Year 1999 (50**  
10          **U.S.C. 1701 note)); or**

11          **(C) impose an embargo on exports**  
12          **to, and imports from, a specific coun-**  
13          **try.**

14          **(2) SPECIFIC DENIALS.—The Secretary**  
15          **of Commerce may prohibit the export of**  
16          **specific encryption products to an indi-**  
17          **vidual or organization in a specific for-**  
18          **ign country or countries identified by**  
19          **the Secretary, if the Secretary, in con-**  
20          **sultation with the Secretary of Defense,**  
21          **the Secretary of State, the Attorney Gen-**  
22          **eral, the Director of the Federal Bureau**  
23          **of Investigation, the Administrator of the**  
24          **Drug Enforcement Administration, and**  
25          **the Director of Central Intelligence, de-**

1 **termines that there is credible evidence**  
2 **that such encryption products will be**  
3 **used—**

4 **(A) for military or terrorist end-**  
5 **use;**

6 **(B) to facilitate the import of il-**  
7 **licit drugs into the United States;**

8 **(C) in the manufacture of weap-**  
9 **ons of mass destruction or otherwise**  
10 **to assist in the proliferation of weap-**  
11 **ons of mass destruction; or**

12 **(D) for illegal activities involving**  
13 **the sexual exploitation of, abuse of,**  
14 **or sexually explicit conduct with mi-**  
15 **nors.**

16 **(3) OTHER EXPORT CONTROLS.—Any**  
17 **encryption product is subject to export**  
18 **controls for any reason other than the ex-**  
19 **istence of encryption capability, includ-**  
20 **ing export controls imposed on high per-**  
21 **formance computers. Nothing in this Act**  
22 **or the amendments made by this Act al-**  
23 **ters the ability of the Secretary of Com-**  
24 **merce to control exports for reasons**  
25 **other than encryption capabilities.**

1           **(4) DEFINITION.—As used in this sub-**  
2           **section and subsection (b), the term**  
3           **“encryption” has the meaning given that**  
4           **term in section 17(g)(5)(A) of the Export**  
5           **Administration Act of 1979, as added by**  
6           **subsection (a) of this section.**

7           **(d) CONTINUATION OF EXPORT ADMINISTRA-**  
8           **TION ACT.—For purposes of carrying out the**  
9           **amendment made by subsection (a), the Ex-**  
10           **port Administration Act of 1979 shall be**  
11           **deemed to be in effect.**

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

13           **(a) COLLECTION OF INFORMATION BY ATTOR-**  
14           **NEY GENERAL.—The Attorney General shall**  
15           **compile, and maintain in classified form, data**  
16           **on the instances in which encryption (as de-**  
17           **finied in section 2801 of title 18, United States**  
18           **Code) has interfered with, impeded, or ob-**  
19           **structed the ability of the Department of Jus-**  
20           **tice to enforce the criminal laws of the United**  
21           **States.**

22           **(b) AVAILABILITY OF INFORMATION TO THE**  
23           **CONGRESS.—The information compiled under**  
24           **subsection (a), including an unclassified sum-**

1 **mary thereof, shall be made available, upon**  
2 **request, to any Member of Congress.**

3 **[SECTION 1. SHORT TITLE.**

4 *【This Act may be cited as the “Protection of National*  
5 *Security and Public Safety Act”.*

6 **[SEC. 2. EXPORTS OF ENCRYPTION.**

7 *【(a) AUTHORITY TO CONTROL EXPORTS.—The Presi-*  
8 *dent shall control the export of all dual-use encryption prod-*  
9 *ucts.*

10 *【(b) AUTHORITY TO DENY EXPORT FOR NATIONAL*  
11 *SECURITY REASONS.—Notwithstanding any provision of*  
12 *this Act, the President may deny the export of any*  
13 *encryption product on the basis that its export is contrary*  
14 *to the national security interests of the United States.*

15 *【(c) DECISIONS NOT SUBJECT TO JUDICIAL RE-*  
16 *VIEW.—Any decision made by the President or his designee*  
17 *with respect to the export of encryption products under this*  
18 *Act shall not be subject to judicial review.*

19 **[SEC. 3. LICENSE EXCEPTION FOR CERTAIN ENCRYPTION**  
20 **PRODUCTS.**

21 *【Encryption products with encryption strength equal*  
22 *to or less than the level identified in section 5 shall be eligi-*  
23 *ble for export under a license exception if—*

24 *【(1) such encryption product is submitted for a*  
25 *1-time technical review;*

1           **[(2)** *such encryption product does not require li-*  
2           *censing under otherwise applicable regulations;*

3           **[(3)** *such encryption product is not intended for*  
4           *a country, end user, or end use that is by regulation*  
5           *ineligible to receive such product, and the encryption*  
6           *product is otherwise qualified for export; and*

7           **[(4)** *the exporter, at the time of submission of*  
8           *the product for technical review, provides the names*  
9           *and addresses of its distribution chain partners.*

10 **[SEC. 4. ONE-TIME PRODUCT REVIEW.**

11           **[The President shall specify the information that must**  
12 *be submitted for the 1-time review referred to in section 3.*

13 **[SEC. 5. ELIGIBILITY LEVELS.**

14           **[(a) INITIAL ELIGIBILITY LEVEL.—***Not later than 180*  
15 *days after the date of the enactment of this Act, the Presi-*  
16 *dent shall notify the Congress of the maximum level of*  
17 *encryption strength that may be exported from the United*  
18 *States under license exception pursuant to section 3 without*  
19 *harm to the national security interests of the United States.*  
20 *Such level shall not become effective until 30 days after such*  
21 *notification.*

22           **[(b) PERIODIC REVIEW OF ELIGIBILITY LEVEL.—***The*  
23 *President shall, at the end of each successive 180-day period*  
24 *after the notice provided to the Congress under subsection*  
25 *(a), notify the Congress of the maximum level of encryption*

1 *strength, which may not be lower than that in effect under*  
2 *this section during that 180-day period, that may be ex-*  
3 *ported from the United States under a license exception*  
4 *pursuant to section 3 without harm to the national security*  
5 *interests of the United States. Such level shall not become*  
6 *effective until 30 days after such notification.*

7 ***[SEC. 6. ENCRYPTION LICENSES REQUIRED.***

8 ***[(a) UNITED STATES PRODUCTS EXCEEDING CER-***  
9 ***TAIN BIT LENGTH.—An export license is required for the***  
10 ***export of any encryption product designed or manufactured***  
11 ***within the United States with an encryption strength ex-***  
12 ***ceeding the maximum level eligible for a license exception***  
13 ***under section 3.***

14 ***[(b) REQUIREMENTS FOR EXPORT LICENSE APPLICA-***  
15 ***TION.—To apply for an export license, the applicant shall***  
16 ***submit—***

17 ***[(1) the product for technical review;***

18 ***[(2) a certification identifying—***

19 ***[(A) the intended end use of the product;***

20 ***and***

21 ***[(B) the expected end user of the product;***

22 ***[(3) in instances where the export is to a dis-***  
23 ***tribution chain partner—***

24 ***[(A) proof that the distribution chain part-***  
25 ***ner has contractually agreed to abide by all laws***

1           *and regulations of the United States concerning*  
2           *the export and reexport of encryption products*  
3           *designed or manufactured within the United*  
4           *States; and*

5                   **[(B)** *the name and address of the distribu-*  
6                   *tion chain partner; and*

7                   **[(4)** *any other information required by the*  
8           *President.*

9           **[(c)** *POST-EXPORT REPORTING.—*

10                   **[(1)** *UNAUTHORIZED USE.—Any exporter of*  
11           *encryption products that are designed or manufac-*  
12           *tured within the United States shall submit a report*  
13           *to the Secretary at any time the exporter has reason*  
14           *to believe that any such product exported pursuant to*  
15           *this section is being diverted to a use or user not ap-*  
16           *proved at the time of export.*

17                   **[(2)** *DISTRIBUTION CHAIN PARTNERS.—All ex-*  
18           *porters of encryption products that are designed and*  
19           *manufactured within the United States, and all dis-*  
20           *tribution chain partners of such exporters, shall sub-*  
21           *mit to the Secretary a report which shall specify—*

22                           **[(A)** *the particular product sold;*

23                           **[(B)** *the name and address of the end user*  
24                   *of the product; and*

25                           **[(C)** *the intended use of the product sold.*

1 **[SEC. 7. WAIVER AUTHORITY.**

2 **[(a) IN GENERAL.**—*The President may by Executive*  
3 *order waive the applicability of any provision of section*  
4 *3 to a person or entity if the President determines that the*  
5 *waiver is necessary to protect the national security interests*  
6 *of the United States. The President shall, not later than*  
7 *15 days after making such determination, submit a report*  
8 *to the committees referred to in subsection (c) that includes*  
9 *the factual basis upon which such determination was made.*  
10 *The report may be in classified format.*

11 **[(b) WAIVERS FOR CERTAIN CLASSES OF END**  
12 **USERS.**—*The President may by Executive order waive the*  
13 *licensing requirements of section 6 for specific classes of end*  
14 *users identified as being eligible for receipt of encryption*  
15 *commodities and software under license exception in section*  
16 *740.17 of title 15, Code of Federal Regulations, as in effect*  
17 *on July 17, 1999. The President shall, not later than 15*  
18 *days after issuing such a waiver, submit a report to the*  
19 *committees referred to in subsection (c) that includes the*  
20 *factual basis upon which such waiver was made. The report*  
21 *may be in classified format.*

22 **[(c) COMMITTEES.**—*The committees referred to in*  
23 *subsections (a) and (b) are the Committee on International*  
24 *Relations, the Committee on Armed Services, and the Per-*  
25 *manent Select Committee on Intelligence of the House of*  
26 *Representatives, and the Committee on Foreign Relations,*

1 *the Committee on Armed Services, and the Select Committee*  
2 *on Intelligence of the Senate.*

3 **[SEC. 8. ENCRYPTION INDUSTRY AND INFORMATION SECUR-**  
4 **RITY BOARD.**

5 **[(a) ENCRYPTION INDUSTRY AND INFORMATION SECUR-**  
6 **RITY BOARD ESTABLISHED.**—*There is hereby established an*  
7 *Encryption Industry and Information Security Board. The*  
8 *Board shall undertake an advisory role for the President*  
9 *on the matter of foreign availability of encryption products.*

10 **[(b) MEMBERSHIP.**—(1) *The Board shall be composed*  
11 *of 12 members, as follows:*

12 **[(A) The Secretary, or the Secretary's designee.**

13 **[(B) The Attorney General, or his or her des-**  
14 *ignee.*

15 **[(C) The Secretary of Defense, or his or her des-**  
16 *ignee.*

17 **[(D) The Director of Central Intelligence, or his**  
18 *or her designee.*

19 **[(E) The Director of the Federal Bureau of In-**  
20 *vestigation, or his or her designee.*

21 **[(F) The Special Assistant to the President for**  
22 *National Security Affairs, or his or her designee, who*  
23 *shall chair the Board.*

24 **[(G) Six representatives from the private sector**  
25 *who have expertise in the development, operation,*

1        *marketing, law, or public policy relating to informa-*  
2        *tion security or technology. Members under this sub-*  
3        *paragraph shall each serve for 5-year terms.*

4        **[(2)** *The six private sector representatives described*  
5        *in paragraph (1)(G) shall be appointed as follows:*

6                    **[(A)** *Two by the Speaker of the House of*  
7                    *Representatives.*

8                    **[(B)** *One by the Minority Leader of the*  
9                    *House of Representatives.*

10                   **[(C)** *Two by the Majority Leader of the*  
11                   *Senate.*

12                   **[(D)** *One by the Minority Leader of the*  
13                   *Senate.*

14        **[(c)** *MEETINGS.—The Board shall meet at such times*  
15        *and in such places as the Secretary may prescribe, but not*  
16        *less frequently than every four months.*

17        **[(d)** *FINDINGS AND RECOMMENDATIONS.—The chair*  
18        *of the Board shall convey the findings and recommendations*  
19        *of the Board to the President and to the Congress within*  
20        *30 days after each meeting of the Board. The recommenda-*  
21        *tions of the Board are not binding upon the President.*

22        **[(e)** *LIMITATION.—The Board shall have no authority*  
23        *to review any export determination made pursuant to this*  
24        *Act.*

1       **[(f) TERMINATION.**—*This section shall cease to be ef-*  
2 *fective 10 years after the date of the enactment of this Act.*

3       **[SEC. 9. MARKET SHARE SURVEY.**

4       **[The Secretary shall, at least once every 6 months,**  
5 *conduct a market share survey of foreign markets for*  
6 *encryption products. The Secretary shall publish the results*  
7 *of the survey in the Federal Register. The publication shall*  
8 *include an assessment of the market share of each foreign*  
9 *encryption product in each market surveyed and a descrip-*  
10 *tion of the general characteristics of each encryption prod-*  
11 *uct.*

12       **[SEC. 10. DEFINITIONS.**

13       **[In this Act:**

14               **[(1) ENCRYPTION.**—*The term “encryption”*  
15 *means the transformation or scrambling of data, for*  
16 *the purpose of protecting such data, from plaintext to*  
17 *an unreadable or incomprehensible format, regardless*  
18 *of the techniques used for such transformation or*  
19 *scrambling and regardless of the medium in which*  
20 *such data occur or can be found.*

21               **[(2) EXPORT AND EXPORTER.**—*The term “ex-*  
22 *port” includes reexport, the term “exporter” includes*  
23 *“reexporter”.*

24               **[(3) SECRETARY.**—*The term “Secretary” means*  
25 *the Secretary of Commerce.]*

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

2       **(a) SHORT TITLE.—This Act may be cited as**  
 3 **the “Encryption for the National Interest Act”.**

4       **(b) TABLE OF CONTENTS.—The table of con-**  
 5 **tents is as follows:**

*Sec. 1. Short title; table of contents.*

*Sec. 2. Statement of policy.*

*Sec. 3. Congressional findings.*

**TITLE I—DOMESTIC USES OF ENCRYPTION**

*Sec. 101. Definitions.*

*Sec. 102. Lawful use of encryption.*

*Sec. 103. Unlawful use of encryption.*

**TITLE II—GOVERNMENT PROCUREMENT**

*Sec. 201. Federal purchases of encryption products.*

*Sec. 202. Networks established with Federal funds.*

*Sec. 203. Government contract authority.*

*Sec. 204. Product labels.*

*Sec. 205. No private mandate.*

*Sec. 206. Exclusion.*

**TITLE III—EXPORTS OF ENCRYPTION**

*Sec. 301. Exports of encryption.*

*Sec. 302. License exception for certain encryption products.*

*Sec. 303. Discretionary authority.*

*Sec. 304. Expedited review authority.*

*Sec. 305. Encryption licenses required.*

*Sec. 306. Encryption Industry and Information Security Board.*

**TITLE IV—LIABILITY LIMITATIONS**

*Sec. 401. Compliance with court order.*

*Sec. 402. Compliance defense.*

*Sec. 403. Good faith defense.*

**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. FBI technical support.*

*Sec. 604. Severability.*

1 **SEC. 2. STATEMENT OF POLICY.**

2 ***It is the policy of the United States to pro-***  
3 ***tect public computer networks through the use***  
4 ***of strong encryption technology, to promote the***  
5 ***export of encryption products developed and***  
6 ***manufactured in the United States, and to pre-***  
7 ***serve public safety and national security.***

8 **SEC. 3. CONGRESSIONAL FINDINGS.**

9 ***The Congress finds the following:***

10 ***(1) Information security technology,***  
11 ***encryption, is—***

12 ***(A) fundamental to secure the flow***  
13 ***of intelligence information to national***  
14 ***policy makers;***

15 ***(B) critical to the President and***  
16 ***national command authority of the***  
17 ***United States;***

18 ***(C) necessary to the Secretary of***  
19 ***State for the development and execu-***  
20 ***tion of the foreign policy of the United***  
21 ***States;***

22 ***(D) essential to the Secretary of***  
23 ***Defense's responsibilities to ensure the***  
24 ***effectiveness of the Armed Forces of***  
25 ***the United States;***

1           ***(E) invaluable to the protection of***  
2           ***the citizens of the United States from***  
3           ***fraud, theft, drug trafficking, child***  
4           ***pornography; kidnapping, and money***  
5           ***laundering; and***

6           ***(F) basic to the protection of the***  
7           ***nation's critical infrastructures, in-***  
8           ***cluding electrical grids, banking and***  
9           ***financial systems, telecommuni-***  
10           ***cations, water supplies, and transpor-***  
11           ***tation.***

12           ***(2) The goal of any encryption legisla-***  
13           ***tion should be to enhance and promote***  
14           ***the global market strength of United***  
15           ***States encryption manufacturers, while***  
16           ***guaranteeing that national security and***  
17           ***public safety obligations of the Govern-***  
18           ***ment can still be accomplished.***

19           ***(3) It is essential to the national secu-***  
20           ***rity interests of the United States that***  
21           ***United States encryption products domi-***  
22           ***nate the global market.***

23           ***(4) Widespread use of unregulated***  
24           ***encryption products poses a significant***

1        *threat to the national security interests of*  
2        *the United States.*

3            (5) *Leaving the national security and*  
4        *public safety responsibilities of the Gov-*  
5        *ernment to the marketplace alone is not*  
6        *consistent with the obligations of the Gov-*  
7        *ernment to protect the public safety and*  
8        *to defend the Nation.*

9            (6) *In order for the United States posi-*  
10       *tion in the global market to benefit the*  
11       *national security interests of the United*  
12       *States, it is imperative that the export of*  
13       *encryption products be subject to a dy-*  
14       *namic and constructive export control re-*  
15       *gime.*

16           (7) *Export of commercial items are*  
17       *best managed through a regulatory struc-*  
18       *ture which has flexibility to address con-*  
19       *stantly changing market conditions.*

20           (8) *Managing sensitive dual-use tech-*  
21       *nologies, such as encryption products, is*  
22       *challenging in any regulatory environ-*  
23       *ment due to the difficulty in balancing*  
24       *competing interests in national security,*  
25       *public safety, privacy, fair competition*

1       *within the industry, and the dynamic na-*  
2       *ture of the technology.*

3           (9) *There is a widespread perception*  
4       *that the executive branch has not ade-*  
5       *quately balanced the equal and com-*  
6       *peting interests of national security, pub-*  
7       *lic safety, privacy, and industry.*

8           (10) *There is a perception that the*  
9       *current encryption export control policy*  
10      *has done more to disadvantage United*  
11      *States business interests than to promote*  
12      *and protect national security and public*  
13      *safety interests.*

14          (11) *A balance can and must be*  
15      *achieved between industry interests, na-*  
16      *tional security, law enforcement require-*  
17      *ments, and privacy needs.*

18          (12) *A court order process should be*  
19      *required for access to plaintext, where*  
20      *and when available, and criminal and*  
21      *civil penalties should be imposed for mis-*  
22      *use of decryption information.*

23          (13) *Timely access to plaintext capa-*  
24      *bility is—*

1           (A) *necessary to thwarting poten-*  
2           *tial terrorist activities;*

3           (B) *extremely useful in the collec-*  
4           *tion of foreign intelligence;*

5           (C) *indispensable to force protec-*  
6           *tion requirements;*

7           (D) *critical to the investigation*  
8           *and prosecution of criminals; and*

9           (E) *both technically and economi-*  
10          *cally possible.*

11          (14) *The United States Government*  
12          *should encourage the development of*  
13          *those products that would provide a capa-*  
14          *bility allowing law enforcement (Federal,*  
15          *State, and local), with a court order only,*  
16          *to gain timely access to the plaintext of ei-*  
17          *ther stored data or data in transit.*

18          (15) *Unless law enforcement has the*  
19          *benefit of such market encouragement,*  
20          *drug traffickers, spies, child pornog-*  
21          *raphers, pedophiles, kidnappers, terror-*  
22          *ists, mobsters, weapons proliferators,*  
23          *fraud schemers, and other criminals will*  
24          *be able to use encryption software to pro-*

1 *tect their criminal activity and hinder the*  
2 *criminal justice system.*

3 *(16) An effective regulatory approach*  
4 *to manage the proliferation of encryption*  
5 *products which have dual-use capabilities*  
6 *must be maintained and greater con-*  
7 *fidence in the ability of the executive*  
8 *branch to preserve and promote the com-*  
9 *petitive advantage of the United States*  
10 *encryption industry in the global market*  
11 *must be provided.*

12 **TITLE I—DOMESTIC USES OF**  
13 **ENCRYPTION**

14 **SEC. 101. DEFINITIONS.**

15 ***For purposes of this Act:***

16 ***(1) ATTORNEY FOR THE GOVERNMENT.—***  
17 ***The term “attorney for the Government”***  
18 ***has the meaning given such term in Rule***  
19 ***54(c) of the Federal Rules of Criminal***  
20 ***Procedure, and also includes any duly au-***  
21 ***thorized attorney of a State who is au-***  
22 ***thorized to prosecute criminal offenses***  
23 ***within such State.***

24 ***(2) AUTHORIZED PARTY.—The term “au-***  
25 ***thorized party” means any person with***

1 *the legal authority to obtain decryption*  
2 *information or plaintext of encrypted*  
3 *data, including communications.*

4 (3) *COMMUNICATIONS.—The term “com-*  
5 *munications” means any wire communica-*  
6 *tions or electronic communications as*  
7 *those terms are defined in paragraphs (1)*  
8 *and (12) of section 2510 of title 18, United*  
9 *States Code.*

10 (4) *COURT OF COMPETENT JURISDIC-*  
11 *TION.—The term “court of competent juris-*  
12 *isdiction” means any court of the United*  
13 *States organized under Article III of the*  
14 *Constitution of the United States, the*  
15 *court organized under the Foreign Intel-*  
16 *ligence Surveillance Act of 1978 (50 U.S.C.*  
17 *1801 et seq.), or a court of general crimi-*  
18 *nal jurisdiction of a State authorized pur-*  
19 *suant to the laws of such State to enter or-*  
20 *ders authorizing searches and seizures.*

21 (5) *DATA NETWORK SERVICE PROVIDER.—*  
22 *The term “data network service provider”*  
23 *means a person offering any service to the*  
24 *general public that provides the users*

1        *thereof with the ability to transmit or re-*  
2        *ceive data, including communications.*

3            (6)        **DECRYPTION.**—*The        term*  
4        *“decryption” means the retransformation*  
5        *or unscrambling of encrypted data, in-*  
6        *cluding communications, to its readable*  
7        *plaintext version. To “decrypt” data, in-*  
8        *cluding communications, is to perform*  
9        *decryption.*

10           (7)        **DECRYPTION INFORMATION.**—*The*  
11        *term “decryption information” means in-*  
12        *formation or technology that enables one*  
13        *to readily retransform or unscramble*  
14        *encrypted data from its unreadable and*  
15        *incomprehensible format to its readable*  
16        *plaintext version.*

17           (8)        **ELECTRONIC STORAGE.**—*The term*  
18        *“electronic storage” has the meaning*  
19        *given that term in section 2510(17) of title*  
20        *18, United States Code.*

21           (9)        **ENCRYPTION.**—*The        term*  
22        *“encryption” means the transformation or*  
23        *scrambling of data, including commu-*  
24        *nications, from plaintext to an*  
25        *unreadable or incomprehensible format,*

1 *regardless of the technique utilized for*  
2 *such transformation or scrambling and*  
3 *irrespective of the medium in which such*  
4 *data, including communications, occur or*  
5 *can be found, for the purposes of pro-*  
6 *tecting the content of such data, includ-*  
7 *ing communications. To “encrypt” data,*  
8 *including communications, is to perform*  
9 *encryption.*

10 (10) *ENCRYPTION PRODUCT.—The term*  
11 *“encryption product” means any software,*  
12 *technology, commodity, or mechanism,*  
13 *that can be used to encrypt or decrypt or*  
14 *has the capability of encrypting or*  
15 *decrypting any data, including commu-*  
16 *nications.*

17 (11) *FOREIGN AVAILABILITY.—The term*  
18 *“foreign availability” has the meaning ap-*  
19 *plied to foreign availability of encryption*  
20 *products subject to controls under the Ex-*  
21 *port Administration Regulations, as in ef-*  
22 *fect on July 1, 1999.*

23 (12) *GOVERNMENT.—The term “Govern-*  
24 *ment” means the Government of the*  
25 *United States and any agency or instru-*

1 *mentality thereof, or the government of*  
2 *any State, and any of its political subdivi-*  
3 *sions.*

4 (13) *INVESTIGATIVE OR LAW ENFORCE-*  
5 *MENT OFFICER.—The term “investigative or*  
6 *law enforcement officer” has the meaning*  
7 *given that term in section 2510(7) of title*  
8 *18, United States Code.*

9 (14) *NATIONAL SECURITY.—The term*  
10 *“national security” means the national*  
11 *defense, intelligence, or foreign policy in-*  
12 *terests of the United States.*

13 (15) *PLAINTEXT.—The term “plaintext”*  
14 *means the readable or comprehensible*  
15 *format of that data, including commu-*  
16 *nications, which has been encrypted.*

17 (16) *PLAINVOICE.—The term*  
18 *“plainvoice” means communication spe-*  
19 *cific plaintext.*

20 (17) *SECRETARY.—The term “Secretary”*  
21 *means the Secretary of Commerce, unless*  
22 *otherwise specifically identified.*

23 (18) *STATE.—The term “State” has the*  
24 *meaning given that term in section*  
25 *2510(3) of title 18, United States Code.*

1           **(19) TELECOMMUNICATIONS CARRIER.—**  
2           *The term “telecommunications carrier”*  
3           *has the meaning given that term in sec-*  
4           *tion 3 of the Communications Act of 1934*  
5           *(47 U.S.C. 153).*

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

15           **(21) UNITED STATES PERSON.—***The term*  
16           *“United States person” means—*

17                   **(A) any citizen of the United**  
18                   **States;**

19                   **(B) any other person organized**  
20                   **under the laws of any State; and**

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

1 *SEC. 102. LAWFUL USE OF ENCRYPTION.*

2 *Except as otherwise provided by this Act or*  
 3 *otherwise provided by law, it shall be lawful*  
 4 *for any person within any State and for any*  
 5 *United States person to use any encryption*  
 6 *product, regardless of encryption algorithm*  
 7 *selected, encryption bit length chosen, or im-*  
 8 *plementation technique or medium used.*

9 *SEC. 103. UNLAWFUL USE OF ENCRYPTION.*

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

13 **“CHAPTER 125—ENCRYPTED DATA,**  
 14 **INCLUDING COMMUNICATIONS**

*“Sec.*

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

*“2802. Privacy protection.*

*“2803. Court order access to plaintext or decryption information.*

*“2804. Notification procedures.*

*“2805. Lawful use of plaintext or decryption information.*

*“2806. Identification of decryption information.*

*“2807. Definitions.*

15 *“§2801. Unlawful use of encryption in furtherance of*  
 16 *a criminal act*

17 *“(a) PROHIBITED ACTS.—Whoever know-*  
 18 *ingly uses encryption in furtherance of the*  
 19 *commission of a criminal offense for which the*

1 *person may be prosecuted in a district court of*  
2 *the United States shall—*

3           “(1) *in the case of a first offense under*  
4 *this section, be imprisoned for not more*  
5 *than 5 years, or fined under this title, or*  
6 *both; and*

7           “(2) *in the case of a second or subse-*  
8 *quent offense under this section, be im-*  
9 *prisoned for not more than 10 years, or*  
10 *fined under this title, or both.*

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

19       “(c) *PROBABLE CAUSE NOT CONSTITUTED BY*  
20 *USE OF ENCRYPTION.—The use of encryption by*  
21 *itself shall not establish probable cause to be-*  
22 *lieve that a crime is being or has been com-*  
23 *mitted.*

1 **“§ 2802. Privacy protection**

2 **“(a) IN GENERAL.—It shall be unlawful for**  
3 **any person to intentionally—**

4 **“(1) obtain or use decryption informa-**  
5 **tion without lawful authority for the pur-**  
6 **pose of decrypting data, including com-**  
7 **munications;**

8 **“(2) exceed lawful authority in**  
9 **decrypting data, including communica-**  
10 **tions;**

11 **“(3) break the encryption code of an-**  
12 **other person without lawful authority for**  
13 **the purpose of violating the privacy or se-**  
14 **curity of that person or depriving that**  
15 **person of any property rights;**

16 **“(4) impersonate another person for**  
17 **the purpose of obtaining decryption infor-**  
18 **mation of that person without lawful au-**  
19 **thority;**

20 **“(5) facilitate or assist in the**  
21 **encryption of data, including communica-**  
22 **tions, knowing that such data, including**  
23 **communications, are to be used in fur-**  
24 **therance of a crime; or**

25 **“(6) disclose decryption information**  
26 **in violation of a provision of this chapter.**

1       “(b) *CRIMINAL PENALTY.—Whoever violates*  
2 *this section shall be imprisoned for not more*  
3 *than 10 years, or fined under this title, or both.*

4       “§2803. *Court order access to plaintext or decryption*  
5                                   *information*

6       “(a) *COURT ORDER.—(1) A court of com-*  
7 *petent jurisdiction shall issue an order, ex*  
8 *parte, granting an investigative or law en-*  
9 *forcement officer timely access to the plaintext*  
10 *of encrypted data, including communications,*  
11 *or requiring any person in possession of*  
12 *decryption information to provide such infor-*  
13 *mation to a duly authorized investigative or*  
14 *law enforcement officer—*

15                   “(A) *upon the application by an attor-*  
16 *ney for the Government that—*

17                                   “(i) *is made under oath or affir-*  
18 *mation by the attorney for the Govern-*  
19 *ment; and*

20                                   “(ii) *provides a factual basis es-*  
21 *tablishing the relevance that the*  
22 *plaintext or decryption information*  
23 *being sought has to a law enforce-*  
24 *ment, foreign counterintelligence, or*  
25 *international terrorism investigation*

1           *then being conducted pursuant to*  
2           *lawful authorities; and*

3           “(B) *if the court finds, in writing, that*  
4           *the plaintext or decryption information*  
5           *being sought is relevant to an ongoing*  
6           *lawful law enforcement, foreign counter-*  
7           *intelligence, or international terrorism in-*  
8           *vestigation and the investigative or law*  
9           *enforcement officer is entitled to such*  
10          *plaintext or decryption information.*

11          “(2) *The order issued by the court under*  
12          *this section shall be placed under seal, except*  
13          *that a copy may be made available to the in-*  
14          *vestigative or law enforcement officer author-*  
15          *ized to obtain access to the plaintext of the*  
16          *encrypted information, or authorized to obtain*  
17          *the decryption information sought in the ap-*  
18          *plication. Such order shall, subject to the noti-*  
19          *fication procedures set forth in section 2804,*  
20          *also be made available to the person respon-*  
21          *sible for providing the plaintext or the*  
22          *decryption information, pursuant to such*  
23          *order, to the investigative or law enforcement*  
24          *officer.*

1       ***“(3) Disclosure of an application made, or***  
2 ***order issued, under this section, is not author-***  
3 ***ized, except as may otherwise be specifically***  
4 ***permitted by this section or another order of***  
5 ***the court.***

6       ***“(b) RECORD OF ACCESS REQUIRED.—(1)***  
7 ***There shall be created an electronic record, or***  
8 ***similar type record, of each instance in which***  
9 ***an investigative or law enforcement officer,***  
10 ***pursuant to an order under this section, gains***  
11 ***access to the plaintext of otherwise encrypted***  
12 ***information, or is provided decryption infor-***  
13 ***mation, without the knowledge or consent of***  
14 ***the owner of the data, including communica-***  
15 ***tions, who is the user of the encryption product***  
16 ***involved.***

17       ***“(2) The court issuing the order under this***  
18 ***section may require that the electronic or simi-***  
19 ***lar type of record described in paragraph (1)***  
20 ***is maintained in a place and a manner that***  
21 ***is not within the custody or control of an inves-***  
22 ***tigative or law enforcement officer gaining the***  
23 ***access or provided the decryption information.***  
24 ***The record shall be tendered to the court, upon***  
25 ***notice from the court.***

1       ***“(3) The court receiving such electronic or***  
2 ***similar type of record described in paragraph***  
3 ***(1) shall make the original and a certified***  
4 ***copy of the record available to the attorney for***  
5 ***the Government making application under***  
6 ***this section, and to the attorney for, or directly***  
7 ***to, the owner of the data, including commu-***  
8 ***nications, who is the user of the encryption***  
9 ***product, pursuant to the notification proce-***  
10 ***dures set forth in section 2804.***

11       ***“(c) AUTHORITY TO INTERCEPT COMMUNICA-***  
12 ***TIONS NOT INCREASED.—Nothing in this chap-***  
13 ***ter shall be construed to enlarge or modify the***  
14 ***circumstances or procedures under which a***  
15 ***Government entity is entitled to intercept or***  
16 ***obtain oral, wire, or electronic communica-***  
17 ***tions or information.***

18       ***“(d) CONSTRUCTION.—This chapter shall be***  
19 ***strictly construed to apply only to a Govern-***  
20 ***ment entity’s ability to decrypt data, including***  
21 ***communications, for which it has previously***  
22 ***obtained lawful authority to intercept or ob-***  
23 ***tain pursuant to other lawful authorities,***  
24 ***which without an order issued under this sec-***  
25 ***tion would otherwise remain encrypted.***

1 *“§2804. Notification procedures*

2 *“(a) IN GENERAL.—Within a reasonable*  
3 *time, but not later than 90 days after the filing*  
4 *of an application for an order under section*  
5 *2803 which is granted, the court shall cause to*  
6 *be served, on the persons named in the order*  
7 *or the application, and such other parties*  
8 *whose decryption information or whose*  
9 *plaintext has been provided to an investigative*  
10 *or law enforcement officer pursuant to this*  
11 *chapter, as the court may determine is in the*  
12 *interest of justice, an inventory which shall in-*  
13 *clude notice of—*

14 *“(1) the fact of the entry of the order*  
15 *or the application;*

16 *“(2) the date of the entry of the appli-*  
17 *cation and issuance of the order; and*

18 *“(3) the fact that the person’s*  
19 *decryption information or plaintext data,*  
20 *including communications, has been pro-*  
21 *vided or accessed by an investigative or*  
22 *law enforcement officer.*

23 *The court, upon the filing of a motion, may*  
24 *make available to that person or that person’s*  
25 *counsel, for inspection, such portions of the*

1 *plaintext, applications, and orders as the*  
2 *court determines to be in the interest of justice.*

3       “(b) *POSTPONEMENT OF INVENTORY FOR*  
4 *GOOD CAUSE.—(1) On an ex parte showing of*  
5 *good cause by an attorney for the Government*  
6 *to a court of competent jurisdiction, the serv-*  
7 *ing of the inventory required by subsection (a)*  
8 *may be postponed for an additional 30 days*  
9 *after the granting of an order pursuant to the*  
10 *ex parte motion.*

11       “(2) *No more than 3 ex parte motions pur-*  
12 *suant to paragraph (1) are authorized.*

13       “(c) *ADMISSION INTO EVIDENCE.—The con-*  
14 *tent of any encrypted information that has*  
15 *been obtained pursuant to this chapter or evi-*  
16 *dence derived therefrom shall not be received*  
17 *in evidence or otherwise disclosed in any trial,*  
18 *hearing, or other proceeding in a Federal or*  
19 *State court, other than the court organized*  
20 *pursuant to the Foreign Intelligence Surveil-*  
21 *lance Act of 1978, unless each party, not less*  
22 *than 10 days before the trial, hearing, or pro-*  
23 *ceeding, has been furnished with a copy of the*  
24 *order, and accompanying application, under*  
25 *which the decryption or access to plaintext*

1 *was authorized or approved. This 10-day pe-*  
2 *riod may be waived by the court if the court*  
3 *finds that it was not possible to furnish the*  
4 *party with the information described in the*  
5 *preceding sentence within 10 days before the*  
6 *trial, hearing, or proceeding and that the*  
7 *party will not be prejudiced by the delay in re-*  
8 *ceiving such information.*

9       “(d) **CONSTRUCTION.**—*The provisions of this*  
10 *chapter shall be construed consistent with—*

11               “(1) *the Classified Information Proce-*  
12 *dures Act (18 U.S.C. App.); and*

13               “(2) *the Foreign Intelligence Surveil-*  
14 *lance Act of 1978 (50 U.S.C. 1801 et seq.).*

15       “(e) **CONTEMPT.**—*Any violation of the provi-*  
16 *sions of this section may be punished by the*  
17 *court as a contempt thereof.*

18       “(f) **MOTION TO SUPPRESS.**—*Any aggrieved*  
19 *person in any trial, hearing, or proceeding in*  
20 *or before any court, department, officer, agen-*  
21 *cy, regulatory body, or other authority of the*  
22 *United States or a State, other than the court*  
23 *organized pursuant to the Foreign Intelligence*  
24 *Surveillance Act of 1978, may move to suppress*  
25 *the contents of any decrypted data, including*

1 *communications, obtained pursuant to this*  
2 *chapter, or evidence derived therefrom, on the*  
3 *grounds that —*

4           “(1) *the plaintext was decrypted or*  
5           *accessed in violation of this chapter;*

6           “(2) *the order of authorization or ap-*  
7           *proval under which it was decrypted or*  
8           *accessed is insufficient on its face; or*

9           “(3) *the decryption was not made in*  
10          *conformity with the order of authoriza-*  
11          *tion or approval.*

12 *Such motion shall be made before the trial,*  
13 *hearing, or proceeding unless there was no op-*  
14 *portunity to make such motion, or the person*  
15 *was not aware of the grounds of the motion.*  
16 *If the motion is granted, the plaintext of the*  
17 *decrypted data, including communications, or*  
18 *evidence derived therefrom, shall be treated as*  
19 *having been obtained in violation of this chap-*  
20 *ter. The court, upon the filing of such motion*  
21 *by the aggrieved person, may make available*  
22 *to the aggrieved person or that person’s coun-*  
23 *sel for inspection such portions of the*  
24 *decrypted plaintext, or evidence derived there-*

1 *from, as the court determines to be in the inter-*  
2 *ests of justice.*

3       “(g) *APPEAL BY UNITED STATES.—In addi-*  
4 *tion to any other right to appeal, the United*  
5 *States shall have the right to appeal from an*  
6 *order granting a motion to suppress made*  
7 *under subsection (f), or the denial of an appli-*  
8 *cation for an order under section 2803, if the*  
9 *attorney for the Government certifies to the*  
10 *court or other official granting such motion or*  
11 *denying such application that the appeal is*  
12 *not taken for purposes of delay. Such appeal*  
13 *shall be taken within 30 days after the date the*  
14 *order was entered on the docket and shall be*  
15 *diligently prosecuted.*

16       “(h) *CIVIL ACTION FOR VIOLATION.—Except*  
17 *as otherwise provided in this chapter, any per-*  
18 *son described in subsection (i) may, in a civil*  
19 *action, recover from the United States Govern-*  
20 *ment the actual damages suffered by the per-*  
21 *son as a result of a violation described in that*  
22 *subsection, reasonable attorney’s fees, and*  
23 *other litigation costs reasonably incurred in*  
24 *prosecuting such claim.*

1       “(i) **COVERED PERSONS.**—*Subsection (h) ap-*  
2 *plies to any person whose decryption*  
3 *information—*

4               “(1) *is knowingly obtained without*  
5 *lawful authority by an investigative or*  
6 *law enforcement officer;*

7               “(2) *is obtained by an investigative or*  
8 *law enforcement officer with lawful au-*  
9 *thority and is knowingly used or disclosed*  
10 *by such officer unlawfully; or*

11               “(3) *is obtained by an investigative or*  
12 *law enforcement officer with lawful au-*  
13 *thority and whose decryption information*  
14 *is unlawfully used to disclose the*  
15 *plaintext of the data, including commu-*  
16 *nications.*

17       “(j) **LIMITATION.**—*A civil action under sub-*  
18 *section (h) shall be commenced not later than*  
19 *2 years after the date on which the unlawful*  
20 *action took place, or 2 years after the date on*  
21 *which the claimant first discovers the viola-*  
22 *tion, whichever is later.*

23       “(k) **EXCLUSIVE REMEDIES.**—*The remedies*  
24 *and sanctions described in this chapter with*  
25 *respect to the decryption of data, including*

1 *communications, are the only judicial rem-*  
2 *edies and sanctions for violations of this chap-*  
3 *ter involving such decryptions, other than vio-*  
4 *lations based on the deprivation of any rights,*  
5 *privileges, or immunities secured by the Con-*  
6 *stitution.*

7       “(l) *TECHNICAL ASSISTANCE BY PROVIDERS.—*  
8 *A provider of encryption technology or network*  
9 *service that has received an order issued by a*  
10 *court pursuant to this chapter shall provide to*  
11 *the investigative or law enforcement officer*  
12 *concerned such technical assistance as is nec-*  
13 *essary to execute the order. Such provider may,*  
14 *however, move the court to modify or quash the*  
15 *order on the ground that its assistance with*  
16 *respect to the decryption or access to plaintext*  
17 *cannot be performed in fact, or in a timely or*  
18 *reasonable fashion. The court, upon notice to*  
19 *the Government, shall decide such motion ex-*  
20 *pedientiously.*

21       “(m) *REPORTS TO CONGRESS.—In May of*  
22 *each year, the Attorney General, or an Assist-*  
23 *ant Attorney General specifically designated*  
24 *by the Attorney General, shall report in writ-*  
25 *ing to Congress on the number of applications*

1 *made and orders entered authorizing Federal,*  
2 *State, and local law enforcement access to*  
3 *decryption information for the purposes of*  
4 *reading the plaintext of otherwise encrypted*  
5 *data, including communications, pursuant to*  
6 *this chapter. Such reports shall be submitted*  
7 *to the Committees on the Judiciary of the*  
8 *House of Representatives and of the Senate,*  
9 *and to the Permanent Select Committee on In-*  
10 *telligence for the House of Representatives and*  
11 *the Select Committee on Intelligence for the*  
12 *Senate.*

13 *“§2805. Lawful use of plaintext or decryption infor-*  
14 *mation*

15 *“(a) AUTHORIZED USE OF DECRYPTION IN-*  
16 *FORMATION.—*

17 *“(1) CRIMINAL INVESTIGATIONS.—An in-*  
18 *vestigative or law enforcement officer to*  
19 *whom plaintext or decryption information*  
20 *is provided may only use such plaintext or*  
21 *decryption information for the purposes of*  
22 *conducting a lawful criminal investiga-*  
23 *tion, foreign counterintelligence, or inter-*  
24 *national terrorism investigation, and for*

1 *the purposes of preparing for and pros-*  
2 *ecuting any criminal violation of law.*

3 *“(2) CIVIL REDRESS.—Any plaintext or*  
4 *decryption information provided under*  
5 *this chapter to an investigative or law en-*  
6 *forcement officer may not be disclosed, ex-*  
7 *cept by court order, to any other person*  
8 *for use in a civil proceeding that is unre-*  
9 *lated to a criminal investigation and*  
10 *prosecution for which the plaintext or*  
11 *decryption information is authorized*  
12 *under paragraph (1). Such order shall*  
13 *only issue upon a showing by the party*  
14 *seeking disclosure that there is no alter-*  
15 *native means of obtaining the plaintext,*  
16 *or decryption information, being sought*  
17 *and the court also finds that the interests*  
18 *of justice would not be served by non-*  
19 *disclosure.*

20 *“(b) LIMITATION.—An investigative or law*  
21 *enforcement officer may not use decryption in-*  
22 *formation obtained under this chapter to de-*  
23 *termine the plaintext of any data, including*  
24 *communications, unless it has obtained lawful*

1 *authority to obtain such data, including com-*  
2 *munications, under other lawful authorities.*

3 **“(c) RETURN OF DECRYPTION INFORMA-**  
4 **TION.—An attorney for the Government shall,**  
5 **upon the issuance of an order of a court of**  
6 **competent jurisdiction—**

7 **“(1)(A) return any decryption informa-**  
8 **tion to the person responsible for pro-**  
9 **viding it to an investigative or law en-**  
10 **forcement officer pursuant to this chap-**  
11 **ter; or**

12 **“(B) destroy such decryption informa-**  
13 **tion, if the court finds that the interests of**  
14 **justice or public safety require that such**  
15 **decryption information should not be re-**  
16 **turned to the provider; and**

17 **“(2) within 10 days after execution of**  
18 **the court’s order to return or destroy the**  
19 **decryption information—**

20 **“(A) certify to the court that the**  
21 **decryption information has either**  
22 **been returned or destroyed consistent**  
23 **with the court’s order; and**

1           “(B) if applicable, notify the pro-  
2           vider of the decryption information of  
3           the destruction of such information.

4           “(d) **OTHER DISCLOSURE OF DECRYPTION IN-**  
5 **FORMATION.—***Except as otherwise provided in*  
6 *section 2803, decryption information or the*  
7 *plaintext of otherwise encrypted data, includ-*  
8 *ing communications, shall not be disclosed by*  
9 *any person unless the disclosure is—*

10           “(1) *to the person encrypting the data,*  
11 *including communications, or an author-*  
12 *ized agent thereof;*

13           “(2) *with the consent of the person*  
14 *encrypting the data, including pursuant*  
15 *to a contract entered into with the person;*

16           “(3) *pursuant to a court order upon a*  
17 *showing of compelling need for the infor-*  
18 *mation that cannot be accommodated by*  
19 *any other means if—*

20           “(A) *the person who supplied the*  
21 *information is given reasonable no-*  
22 *tice, by the person seeking the disclo-*  
23 *sure, of the court proceeding relevant*  
24 *to the issuance of the court order; and*

1           “(B) *the person who supplied the*  
2           *information is afforded the oppor-*  
3           *tunity to appear in the court pro-*  
4           *ceeding and contest the claim of the*  
5           *person seeking the disclosure;*

6           “(4) *pursuant to a determination by a*  
7           *court of competent jurisdiction that an-*  
8           *other person is lawfully entitled to hold*  
9           *such decryption information, including*  
10          *determinations arising from legal pro-*  
11          *ceedings associated with the incapacity,*  
12          *death, or dissolution of any person; or*

13          “(5) *otherwise permitted by law.*

14          “§2806. *Identification of decryption information*

15          “(a) *IDENTIFICATION.—To avoid inadvertent*  
16          *disclosure of decryption information, any per-*  
17          *son who provides decryption information to an*  
18          *investigative or law enforcement officer pursu-*  
19          *ant to this chapter shall specifically identify*  
20          *that part of the material that discloses*  
21          *decryption information as such.*

22          “(b) *RESPONSIBILITY OF INVESTIGATIVE OR*  
23          *LAW ENFORCEMENT OFFICER.—The investigative*  
24          *or law enforcement officer receiving any*  
25          *decryption information under this chapter*

1 *shall maintain such information in a facility*  
 2 *and in a method so as to reasonably assure*  
 3 *that inadvertent disclosure does not occur.*

4 “§2807. *Definitions*

5 “*The definitions set forth in section 101 of*  
 6 *the Encryption for the National Interest Act*  
 7 *shall apply to this chapter.*”.

8 (b) *CONFORMING AMENDMENT.—The table of*  
 9 *chapters for part I of title 18, United States*  
 10 *Code, is amended by inserting after the item*  
 11 *relating to chapter 121 the following new item:*  
 “125. *Encrypted data, including communications ..... 2801*”.

12 **TITLE II—GOVERNMENT**  
 13 **PROCUREMENT**

14 *SEC. 201. FEDERAL PURCHASES OF ENCRYPTION PROD-*  
 15 *UCTS.*

16 (a) *DECRYPTION CAPABILITIES.—The Presi-*  
 17 *dent may, consistent with the provisions of*  
 18 *subsection (b), direct that any encryption*  
 19 *product or service purchased or otherwise pro-*  
 20 *cured by the United States Government to pro-*  
 21 *vide the security service of data confidentiality*  
 22 *for a computer system owned and operated by*  
 23 *the United States Government shall include*  
 24 *recoverability features or functions that en-*  
 25 *able the timely decryption of encrypted data,*

1 *including communications, or timely access to*  
2 *plaintext by an authorized party without the*  
3 *knowledge or cooperation of the person using*  
4 *such encryption products or services.*

5       **(b) CONSISTENCY WITH INTELLIGENCE SERV-**  
6 **ICES AND MILITARY OPERATIONS.—***The President*  
7 *shall ensure that all encryption products pur-*  
8 *chased or used by the United States Govern-*  
9 *ment are supportive of, and consistent with,*  
10 *all statutory obligations to protect sources and*  
11 *methods of intelligence collection and activi-*  
12 *ties, and supportive of, and consistent with,*  
13 *those needs required for military operations*  
14 *and the conduct of foreign policy.*

15 **SEC. 202. NETWORKS ESTABLISHED WITH FEDERAL FUNDS.**

16       *The President may direct that any commu-*  
17 *nications network established for the purpose*  
18 *of conducting the business of the Federal Gov-*  
19 *ernment shall use encryption products that—*

20           **(1) include features and functions**  
21 *that enable the timely decryption of*  
22 *encrypted data, including communica-*  
23 *tions, or timely access to plaintext, by an*  
24 *authorized party without the knowledge*

1 *or cooperation of the person using such*  
2 *encryption products or services; and*

3 *(2) are supportive of, and consistent*  
4 *with, all statutory obligations to protect*  
5 *sources and methods of intelligence col-*  
6 *lection and activities, and supportive of,*  
7 *and consistent with, those needs required*  
8 *for military operations and the conduct of*  
9 *foreign policy.*

10 *SEC. 203. GOVERNMENT CONTRACT AUTHORITY.*

11 *The President may require as a condition*  
12 *of any contract by the Government with a pri-*  
13 *vate sector vendor that any encryption product*  
14 *used by the vendor in carrying out the provi-*  
15 *sions of the contract with the Government in-*  
16 *clude features and functions that enable the*  
17 *timely decryption of encrypted data, including*  
18 *communications, or timely access to plaintext,*  
19 *by an authorized party without the knowledge*  
20 *or cooperation of the person using such*  
21 *encryption products or services.*

22 *SEC. 204. PRODUCT LABELS.*

23 *An encryption product may be labeled to*  
24 *inform Government users that the product is*  
25 *authorized for sale to or for use by Government*

1 *agencies or Government contractors in trans-*  
2 *actions and communications with the United*  
3 *States Government under this title.*

4 *SEC. 205. NO PRIVATE MANDATE.*

5 *The United States Government may not re-*  
6 *quire the use of encryption standards for the*  
7 *private sector except as otherwise authorized*  
8 *by section 204.*

9 *SEC. 206. EXCLUSION.*

10 *Nothing in this title shall apply to*  
11 *encryption products and services used solely*  
12 *for access control, authentication, integrity,*  
13 *nonrepudiation, digital signatures, or other*  
14 *similar purposes.*

15 **TITLE III—EXPORTS OF**  
16 **ENCRYPTION**

17 *SEC. 301. EXPORTS OF ENCRYPTION.*

18 *(a) AUTHORITY TO CONTROL EXPORTS.—The*  
19 *President shall control the export of all dual-*  
20 *use encryption products.*

21 *(b) AUTHORITY TO DENY EXPORT FOR NA-*  
22 *TIONAL SECURITY REASONS.—Notwithstanding*  
23 *any provision of this title, the President may*  
24 *deny the export of any encryption product on*

1 *the basis that its export is contrary to the na-*  
2 *tional security.*

3       **(c) DECISIONS NOT SUBJECT TO JUDICIAL RE-**  
4 **VIEW.**—*Any decision made by the President or*  
5 *his designee with respect to the export of*  
6 *encryption products under this title shall not*  
7 *be subject to judicial review.*

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

10       **(a) LICENSE EXCEPTION.**—*Upon the enact-*  
11 *ment of this Act, any encryption product with*  
12 *an encryption strength of 64 bits or less shall*  
13 *be eligible for export under a license exception*  
14 *if—*

15               **(1) such encryption product is sub-**  
16 **mitted for a 1-time technical review;**

17               **(2) such encryption product does not**  
18 **require licensing under otherwise appli-**  
19 **cable regulations;**

20               **(3) such encryption product is not in-**  
21 **tended for a country, end user, or end use**  
22 **that is by regulation ineligible to receive**  
23 **such product, and the encryption product**  
24 **is otherwise qualified for export;**

1           ***(4) the exporter, within 180 days after***  
2           ***the export of the product, submits a cer-***  
3           ***tification identifying—***

4                   ***(A) the intended end use of the***  
5                   ***product; and***

6                   ***(B) the name and address of the***  
7                   ***intended recipient of the product,***  
8                   ***where available;***

9           ***(5) the exporter, within 180 days of the***  
10           ***export of the product, provides the names***  
11           ***and addresses of its distribution chain***  
12           ***partners; and***

13           ***(6) the exporter, at the time of submis-***  
14           ***sion of the product for technical review,***  
15           ***provides proof that its distribution chain***  
16           ***partners have contractually agreed to***  
17           ***abide by all laws and regulations of the***  
18           ***United States concerning the export and***  
19           ***reexport of encryption products designed***  
20           ***or manufactured within the United***  
21           ***States.***

22           ***(b) ONE-TIME TECHNICAL REVIEW.—(1) The***  
23           ***technical review referred to in subsection (a)***  
24           ***shall be completed within no longer than 45***

1 *days after the submission of all of the informa-*  
2 *tion required under paragraph (2).*

3 *(2) The President shall specify the infor-*  
4 *mation that must be submitted for the 1-time*  
5 *technical review referred to in this section.*

6 *(3) An encryption product may not be ex-*  
7 *ported during the technical review of that*  
8 *product under this section.*

9 *(c) PERIODIC REVIEW OF LICENSE EXCEPTION*  
10 *ELIGIBILITY LEVEL.—(1) Not later than 180 days*  
11 *after the date of the enactment of this Act, the*  
12 *President shall notify the Congress of the max-*  
13 *imum level of encryption strength, which may*  
14 *not be lower than 64-bit, that may be exported*  
15 *from the United States under license exception*  
16 *pursuant to this section consistent with the*  
17 *national security.*

18 *(2) The President shall, at the end of each*  
19 *successive 180-day period after the notice pro-*  
20 *vided to the Congress under paragraph (1), no-*  
21 *tify the Congress of the maximum level of*  
22 *encryption strength, which may not be lower*  
23 *than that in effect under this section during*  
24 *that 180-day period, that may be exported from*  
25 *the United States under a license exception*

1 *pursuant to this section consistent with the*  
2 *national security.*

3 **(d) FACTORS NOT TO BE CONSIDERED.**—A li-  
4 *cence exception for the exports of an*  
5 *encryption product under this section may be*  
6 *allowed whether or not the product contains a*  
7 *method of decrypting encrypted data.*

8 **SEC. 303. DISCRETIONARY AUTHORITY.**

9 *Notwithstanding the requirements of sec-*  
10 *tion 305, the President may permit the export,*  
11 *under a license exception pursuant to the con-*  
12 *ditions of section 302, of encryption products*  
13 *with an encryption strength exceeding the*  
14 *maximum level eligible for a license exception*  
15 *under section 302, if the export is consistent*  
16 *with the national security.*

17 **SEC. 304. EXPEDITED REVIEW AUTHORITY.**

18 *The President shall establish procedures*  
19 *for the expedited review of commodity classi-*  
20 *fication requests, or export license applica-*  
21 *tions, involving encryption products that are*  
22 *specifically approved, by regulation, for ex-*  
23 *port.*

1 *SEC. 305. ENCRYPTION LICENSES REQUIRED.*

2       ***(a) UNITED STATES PRODUCTS EXCEEDING***  
3 ***CERTAIN BIT LENGTH.—Except as permitted***  
4 ***under section 303, in the case of all encryption***  
5 ***products with an encryption strength exceed-***  
6 ***ing the maximum level eligible for a license ex-***  
7 ***ception under section 302, which are designed***  
8 ***or manufactured within the United States, the***  
9 ***President may grant a license for export of***  
10 ***such encryption products, under the following***  
11 ***conditions:***

12           ***(1) There shall not be any require-***  
13 ***ment, as a basis for an export license, that***  
14 ***a product contains a method of—***

15                   ***(A) gaining timely access to***  
16 ***plaintext; or***

17                   ***(B) gaining timely access to***  
18 ***decryption information.***

19           ***(2) The export license applicant shall***  
20 ***submit—***

21                   ***(A) the product for technical re-***  
22 ***view;***

23                   ***(B) a certification, under oath,***  
24 ***identifying—***

25                           ***(i) the intended end use of the***  
26 ***product; and***

1                   (ii) *the expected end user or*  
2                   *class of end users of the product;*

3                   (C) *proof that its distribution*  
4                   *chain partners have contractually*  
5                   *agreed to abide by all laws and regu-*  
6                   *lations of the United States con-*  
7                   *cerning the export and reexport of*  
8                   *encryption products designed or man-*  
9                   *ufactured within the United States;*  
10                  *and*

11                  (D) *the names and addresses of its*  
12                  *distribution chain partners.*

13                  (b) **TECHNICAL REVIEW FOR LICENSE APPLI-**  
14 **CANTS.—**(1) *The technical review described in*  
15 *subsection (a)(3)(A) shall be completed within*  
16 *45 days after the submission of all the infor-*  
17 *mation required under paragraph (2).*

18                  (2) *The information to be submitted for the*  
19 *technical review shall be the same as that re-*  
20 *quired to be submitted pursuant to section*  
21 *302(b)(2).*

22                  (3) *An encryption product may not be ex-*  
23 *ported during the technical review of that*  
24 *product under this section.*

25                  (c) **POST-EXPORT REPORTING.—**

1           **(1) UNAUTHORIZED USE.**—*All exporters*  
2           *of encryption products that are designed*  
3           *or manufactured within the United States*  
4           *shall submit a report to the Secretary at*  
5           *any time the exporter has reason to be-*  
6           *lieve any such exported product is being*  
7           *diverted to a use or a user not approved*  
8           *at the time of export.*

9           **(2) PIRATING.**—*All exporters of*  
10          *encryption products that are designed or*  
11          *manufactured within the United States*  
12          *shall report any pirating of their tech-*  
13          *nology or intellectual property to the Sec-*  
14          *retary as soon as practicable after dis-*  
15          *covery.*

16          **(3) DISTRIBUTION CHAIN PARTNERS.**—*All*  
17          *exporters of encryption products that are*  
18          *designed or manufactured within the*  
19          *United States, and all distribution chain*  
20          *partners of such exporters, shall submit to*  
21          *the Secretary a report which shall*  
22          *specify—*

23                   **(A) the particular product sold;**

24                   **(B) the name and address of—**

1                   *(i) the ultimate end user of the*  
2                   *product, if known; or*

3                   *(ii) the name and address of*  
4                   *the next purchaser in the distribu-*  
5                   *tion chain; and*

6                   *(C) the intended use of the product*  
7                   *sold.*

8           ***(d) EXERCISE OF OTHER AUTHORITIES.—The***  
9           ***Secretary, the Secretary of Defense, and the***  
10           ***Secretary of State may exercise the authorities***  
11           ***they have under other provisions of law, in-***  
12           ***cluding the Export Administration Act of 1979,***  
13           ***as continued in effect under the International***  
14           ***Emergency Economic Powers Act, to carry out***  
15           ***this title.***

16           ***(e) WAIVER AUTHORITY.—***

17                   ***(1) IN GENERAL.—The President may by***  
18                   ***Executive order waive any provision of***  
19                   ***this title, or the applicability of any such***  
20                   ***provision to a person or entity, if the***  
21                   ***President determines that the waiver is***  
22                   ***necessary to advance the national secu-***  
23                   ***rity. The President shall, not later than 15***  
24                   ***days after making such determination,***  
25                   ***submit a report to the committees referred***

1 *to in paragraph (2) that includes the fac-*  
2 *tual basis upon which such determination*  
3 *was made. The report may be in classified*  
4 *format.*

5 (2) *COMMITTEES.—The committees re-*  
6 *ferred to in paragraph (1) are the Com-*  
7 *mittee on International Relations, the*  
8 *Committee on Armed Services, and the*  
9 *Permanent Select Committee on Intel-*  
10 *ligence of the House of Representatives,*  
11 *and the Committee on Foreign Relations,*  
12 *the Committee on Armed Services, and the*  
13 *Select Committee on Intelligence of the*  
14 *Senate.*

15 (3) *DECISIONS NOT SUBJECT TO JUDICIAL*  
16 *REVIEW.—Any determination made by the*  
17 *President under this subsection shall not*  
18 *be subject to judicial review.*

19 *SEC. 306. ENCRYPTION INDUSTRY AND INFORMATION SE-*  
20 *CURITY BOARD.*

21 (a) *ENCRYPTION INDUSTRY AND INFORMA-*  
22 *TION SECURITY BOARD ESTABLISHED.—There is*  
23 *hereby established an Encryption Industry*  
24 *and Information Security Board. The Board*

1 *shall undertake an advisory role for the Presi-*  
2 *dent.*

3 **(b) PURPOSES.—***The purposes of the Board*  
4 *are—*

5 *(1) to provide a forum to foster com-*  
6 *munication and coordination between in-*  
7 *dustry and the Federal Government on*  
8 *matters relating to the use of encryption*  
9 *products;*

10 *(2) to enable the United States to ef-*  
11 *fectively and continually understand the*  
12 *benefits and risks to its national security,*  
13 *law enforcement, and public safety inter-*  
14 *ests by virtue of the proliferation of strong*  
15 *encryption on the global market;*

16 *(3) to evaluate and make rec-*  
17 *ommendations regarding the further de-*  
18 *velopment and use of encryption;*

19 *(4) to advance the development of*  
20 *international standards regarding inter-*  
21 *operability and global use of encryption*  
22 *products;*

23 *(5) to promote the export of encryption*  
24 *products manufactured in the United*  
25 *States;*

1           ***(6) to recommend policies enhancing***  
2           ***the security of public networks;***

3           ***(7) to encourage research and devel-***  
4           ***opment of products that will foster elec-***  
5           ***tronic commerce;***

6           ***(8) to promote the protection of intel-***  
7           ***lectual property and privacy rights of in-***  
8           ***dividuals using public networks; and***

9           ***(9) to evaluate the availability and***  
10           ***market share of foreign encryption prod-***  
11           ***ucts and their threat to United States in-***  
12           ***dustry.***

13           ***(c) MEMBERSHIP.—(1) The Board shall be***  
14           ***composed of 12 members, as follows:***

15           ***(A) The Secretary, or the Secretary's***  
16           ***designee.***

17           ***(B) The Attorney General, or his or***  
18           ***her designee.***

19           ***(C) The Secretary of Defense, or the***  
20           ***Secretary's designee.***

21           ***(D) The Director of Central Intel-***  
22           ***ligence, or his or her designee.***

23           ***(E) The Director of the Federal Bu-***  
24           ***reau of Investigation, or his or her des-***  
25           ***ignee.***

1           ***(F) The Special Assistant to the Presi-***  
2           ***dent for National Security Affairs, or his***  
3           ***or her designee, who shall chair the***  
4           ***Board.***

5           ***(G) Six representatives from the pri-***  
6           ***ivate sector who have expertise in the de-***  
7           ***velopment, operation, marketing, law, or***  
8           ***public policy relating to information secu-***  
9           ***rity or technology. Members under this***  
10          ***subparagraph shall each serve for 5-year***  
11          ***terms.***

12          ***(2) The six private sector representatives***  
13          ***described in paragraph (1)(G) shall be ap-***  
14          ***pointed as follows:***

15                 ***(A) Two by the Speaker of the***  
16                 ***House of Representatives.***

17                 ***(B) One by the Minority Leader of***  
18                 ***the House of Representatives.***

19                 ***(C) Two by the Majority Leader of***  
20                 ***the Senate.***

21                 ***(D) One by the Minority Leader of***  
22                 ***the Senate.***

23          ***(e) MEETINGS.—The Board shall meet at***  
24          ***such times and in such places as the Secretary***  
25          ***may prescribe, but not less frequently than***

1 *every four months. The Federal Advisory Com-*  
2 *mittee Act (5 U.S.C. App.) does not apply to the*  
3 *Board or to meetings held by the Board under*  
4 *this section.*

5       **(f) FINDINGS AND RECOMMENDATIONS.**—*The*  
6 *chair of the Board shall convey the findings*  
7 *and recommendations of the Board to the*  
8 *President and to the Congress within 30 days*  
9 *after each meeting of the Board. The rec-*  
10 *ommendations of the Board are not binding*  
11 *upon the President.*

12       **(g) LIMITATION.**—*The Board shall have no*  
13 *authority to review any export determination*  
14 *made pursuant to this title.*

15       **(h) FOREIGN AVAILABILITY.**—*The consider-*  
16 *ation of foreign availability by the Board shall*  
17 *include computer software that is distributed*  
18 *over the Internet or advertised for sale, license,*  
19 *or transfer, including over-the-counter retail*  
20 *sales, mail order transactions, telephone order*  
21 *transactions, electronic distribution, or sale*  
22 *on approval and its comparability with United*  
23 *States products and its use in United States*  
24 *and foreign markets.*

1       ***(i) TERMINATION.—This section shall cease***  
2 ***to be effective 10 years after the date of the en-***  
3 ***actment of this Act.***

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

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

7       ***(a) NO LIABILITY FOR COMPLIANCE.—Subject***  
8 ***to subsection (b), no civil or criminal liability***  
9 ***under this Act, or under any other provision***  
10 ***of law, shall attach to any person for dis-***  
11 ***closing or providing—***

12               ***(1) the plaintext of encrypted data, in-***  
13 ***cluding communications;***

14               ***(2) the decryption information of such***  
15 ***encrypted data, including communica-***  
16 ***tions; or***

17               ***(3) technical assistance for access to***  
18 ***the plaintext of, or decryption information***  
19 ***for, encrypted data, including commu-***  
20 ***nications.***

21       ***(b) EXCEPTION.—Subsection (a) shall not***  
22 ***apply to a person who provides plaintext or***  
23 ***decryption information to another in violation***  
24 ***of the provisions of this Act.***

1 *SEC. 402. COMPLIANCE DEFENSE.*

2 *Compliance with the provisions of sections*  
3 *2803, 2804, 2805, or 2806 of title 18, United*  
4 *States Code, as added by section 103(a) of this*  
5 *Act, or any regulations authorized by this Act,*  
6 *shall provide a complete defense for any civil*  
7 *action for damages based upon activities cov-*  
8 *ered by this Act, other than an action founded*  
9 *on contract.*

10 *SEC. 403. GOOD FAITH DEFENSE.*

11 *An objectively reasonable reliance on the*  
12 *legal authority provided by this Act and the*  
13 *amendments made by this Act, authorizing ac-*  
14 *cess to the plaintext of otherwise encrypted*  
15 *data, including communications, or to*  
16 *decryption information that will allow the*  
17 *timely decryption of data, including commu-*  
18 *nications, that is otherwise encrypted, shall be*  
19 *an affirmative defense to any criminal or civil*  
20 *action that may be brought under the laws of*  
21 *the United States or any State.*

22 **TITLE V—INTERNATIONAL**  
23 **AGREEMENTS**

24 *SEC. 501. SENSE OF CONGRESS.*

25 *It is the sense of Congress that—*

1           ***(1) the President should conduct nego-***  
2           ***tiations with foreign governments for the***  
3           ***purposes of establishing binding export***  
4           ***control requirements on strong non-***  
5           ***recoverable encryption products; and***

6           ***(2) such agreements should safeguard***  
7           ***the privacy of the citizens of the United***  
8           ***States, prevent economic espionage, and***  
9           ***enhance the information security needs of***  
10          ***the United States.***

11 ***SEC. 502. FAILURE TO NEGOTIATE.***

12          ***The President may consider a govern-***  
13          ***ment's refusal to negotiate agreements de-***  
14          ***scribed in section 501 when considering the***  
15          ***participation of the United States in any co-***  
16          ***operation or assistance program with that***  
17          ***country.***

18 ***SEC. 503. REPORT TO CONGRESS.***

19          ***(a) REPORT TO CONGRESS.—The President***  
20          ***shall report annually to the Congress on the***  
21          ***status of the international effort outlined by***  
22          ***section 501.***

23          ***(b) FIRST REPORT.—The first report re-***  
24          ***quired under subsection (a) shall be submitted***

1 *in unclassified form no later than September*  
2 *1, 2000.*

3 ***TITLE VI—MISCELLANEOUS***  
4 ***PROVISIONS***

5 ***SEC. 601. EFFECT ON LAW ENFORCEMENT ACTIVITIES.***

6 ***(a) COLLECTION OF INFORMATION BY ATTOR-***  
7 ***NEY GENERAL.—The Attorney General shall***  
8 ***compile, and maintain in classified form, data***  
9 ***on—***

10 ***(1) the instances in which encryption***  
11 ***has interfered with, impeded, or ob-***  
12 ***structed the ability of the Department of***  
13 ***Justice to enforce the laws of the United***  
14 ***States; and***

15 ***(2) the instances where the Depart-***  
16 ***ment of Justice has been successful in***  
17 ***overcoming any encryption encountered in***  
18 ***an investigation.***

19 ***(b) AVAILABILITY OF INFORMATION TO THE***  
20 ***CONGRESS.—The information compiled under***  
21 ***subsection (a), including an unclassified sum-***  
22 ***mary thereof, shall be submitted to Congress***  
23 ***annually beginning October 1, 2000.***

1 **SEC. 602. INTERPRETATION.**

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

5 ***(1) preempt or otherwise affect the ap-***  
6 ***plication of the Arms Export Control Act***  
7 ***(22 U.S.C. 2751 et seq.), the Export Admin-***  
8 ***istration Act of 1979 (50 U.S.C. App. 2401***  
9 ***et seq.), or the International Emergency***  
10 ***Economic Powers Act (50 U.S.C. 1701 et***  
11 ***seq.) or any regulations promulgated***  
12 ***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. FBI TECHNICAL SUPPORT.**

19 ***There are authorized to be appropriated***  
20 ***for the Technical Support Center in the Fed-***  
21 ***eral Bureau of Investigation, established pur-***  
22 ***suant to section 811(a)(1) of the Antiterrorism***  
23 ***and Effective Death Penalty Act of 1996 (Pub-***  
24 ***lic Law 104–132)—***

25 ***(1) \$25,000,000 for fiscal year 2000 for***  
26 ***building and personnel costs;***

1           **(2) \$20,000,000 for fiscal year 2001 for**  
2           **personnel and equipment costs;**

3           **(3) \$15,000,000 for fiscal year 2002;**  
4           **and**

5           **(4) \$15,000,000 for fiscal year 2003.**

6 **SEC. 604. SEVERABILITY.**

7           ***If any provision of this Act or the amend-***  
8           ***ments made by this Act, or the application***  
9           ***thereof, to any person or circumstances is held***  
10           ***invalid by a court of the United States, the re-***  
11           ***mainder of this Act or such amendments, and***  
12           ***the application thereof, to other persons or cir-***  
13           ***cumstances shall not be affected thereby.***

Amend the title so as to read: “A bill to protect national security and public safety through the balanced use of export controls on encryption products.”.