

.....
(Original Signature of Member)

106TH CONGRESS
1ST SESSION

H. R. _____

IN THE HOUSE OF REPRESENTATIVES

Mr. GOODLATTE introduced the following bill; which was referred to the
Committee on _____

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”.

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

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

5 **“CHAPTER 125—ENCRYPTED WIRE AND**
6 **ELECTRONIC INFORMATION**

“2801. Definitions.

“2802. Freedom to use encryption.

“2803. Freedom to sell encryption.

“2804. Prohibition on mandatory key escrow.

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

7 **“§ 2801. Definitions**

8 “As used in this chapter—

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

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

17 “(3) the terms ‘encrypt’, ‘encrypted’, and
18 ‘encryption’ mean the scrambling of wire commu-
19 nications, electronic communications, or electroni-
20 cally stored information, using mathematical for-
21 mulas or algorithms in order to preserve the con-
22 fidentiality, integrity, or authenticity of, and prevent

1 unauthorized recipients from accessing or altering,
2 such communications or information;

3 “(4) the term ‘key’ means the variable informa-
4 tion used in a mathematical formula, code, or algo-
5 rithm, or any component thereof, used to decrypt
6 wire communications, electronic communications, or
7 electronically stored information, that has been
8 encrypted; and

9 “(5) the term ‘key recovery information’ means
10 information that would enable obtaining the key of
11 a user of encryption;

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

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

17 “(A) any United States citizen;

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

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

1 **“§ 2802. Freedom to use encryption**

2 “Subject to section 2805, it shall be lawful for any
3 person within any State, and for any United States person
4 in a foreign country, to use any encryption, regardless of
5 the encryption algorithm selected, encryption key length
6 chosen, or implementation technique or medium used.

7 **“§ 2803. Freedom to sell encryption**

8 “Subject to section 2805, it shall be lawful for any
9 person within any State to sell in interstate commerce any
10 encryption, regardless of the encryption algorithm se-
11 lected, encryption key length chosen, or implementation
12 technique or medium used.

13 **“§ 2804. Prohibition on mandatory key escrow**

14 “(a) GENERAL PROHIBITION.—Neither the Federal
15 Government nor a State may require that, or condition
16 any approval on a requirement that, a key, access to a
17 key, key recovery information, or any other plaintext ac-
18 cess capability be—

19 “(1) built into computer hardware or software
20 for any purpose;

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

25 “(3) retained by the owner or user of an
26 encryption key or any other person, other than for

1 encryption products for use by the Federal Govern-
2 ment or a State.

3 “(b) PROHIBITION ON LINKAGE OF DIFFERENT
4 USES OF ENCRYPTION.—Neither the Federal Government
5 nor a State may—

6 “(1) require the use of encryption products,
7 standards, or services used for confidentiality pur-
8 poses, as a condition of the use of such products,
9 standards, or services for authenticity or integrity
10 purposes; or

11 “(2) require the use of encryption products,
12 standards, or services used for authenticity or integ-
13 rity purposes, as a condition of the use of such prod-
14 ucts, standards, or services for confidentiality pur-
15 poses.】

16 “(c) EXCEPTION FOR ACCESS FOR LAW ENFORCE-
17 MENT PURPOSES.—Subsection (a) shall not affect the au-
18 thority of any investigative or law enforcement officer, or
19 any member of the intelligence community as defined in
20 section 3 of the National Security Act of 1947 (50 U.S.C.
21 401a), acting under any law in effect on the effective date
22 of this chapter, to gain access to encrypted communica-
23 tions or information.

1 **“§ 2805. Unlawful use of encryption in furtherance of**
2 **a criminal act**

3 “(a) ENCRYPTION OF INCRIMINATING COMMUNICA-
4 TIONS OR INFORMATION UNLAWFUL.—Any person who,
5 in the commission of a felony under a criminal statute of
6 the United States, knowingly and willfully encrypts in-
7 criminating communications or information relating to
8 that felony with the intent to conceal such communications
9 or information for the purpose of avoiding detection by
10 law enforcement agencies or prosecution—

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

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

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

23 (b) CONFORMING AMENDMENT.—The table of chap-
24 ters for part I of title 18, United States Code, is amended

1 by inserting after the item relating to chapter 123 the fol-
2 lowing new item:

“125. Encrypted wire and electronic information 2801”.

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

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

8 “(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS,
9 AND RELATED EQUIPMENT.—

10 “(1) GENERAL RULE.—Subject to paragraphs
11 (2) and (3), the Secretary shall have exclusive au-
12 thority to control exports of all computer hardware,
13 software, computing devices, customer premises
14 equipment, communications network equipment, and
15 technology for information security (including
16 encryption), except that which is specifically de-
17 signed or modified for military use, including com-
18 mand, control, and intelligence applications.

19 “(2) ITEMS NOT REQUIRING LICENSES.—After
20 a one-time, 15-day technical review by the Secretary,
21 no export license may be required, except pursuant
22 to the Trading with the enemy Act or the Inter-
23 national Emergency Economic Powers Act (but only
24 to the extent that the authority of such Act is not

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

3 “(A) any computer hardware or software
4 or computing device, including computer hard-
5 ware or software or computing devices with
6 encryption capabilities—

7 “(i) that is generally available;

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

14 “(iii) that is used in a commercial,
15 off-the-shelf, consumer product or any
16 component or subassembly designed for
17 use in such a consumer product available
18 within the United States or abroad
19 which—

20 “(I) includes encryption capabili-
21 ties which are inaccessible to the end
22 user; and

23 “(II) is not designed for military
24 or intelligence end use;

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

3 “(i) computer hardware or software
4 (including computer hardware or software
5 with encryption capabilities) that is ex-
6 emptioned from any requirement for a license
7 under subparagraph (A); or

8 “(ii) computer hardware or software
9 that is no more technically complex in its
10 encryption capabilities than computer
11 hardware or software that is exemptioned
12 from any requirement for a license under
13 subparagraph (A) but is not designed for
14 installation by the purchaser;

15 “(C) any computer hardware or software
16 or computing device solely on the basis that it
17 incorporates or employs in any form interface
18 mechanisms for interaction with other computer
19 hardware or software or computing devices, in-
20 cluding computer hardware and software and
21 computing devices with encryption capabilities;

22 “(D) any computing or telecommunication
23 device which incorporates or employs in any
24 form computer hardware or software encryption
25 capabilities which—

1 “(i) are not directly available to the
2 end user; or

3 “(ii) limit the encryption to be point-
4 to-point from the user to a central commu-
5 nications point or link and does not enable
6 end-to-end user encryption;

7 “(E) technical assistance and technical
8 data used for the installation or maintenance of
9 computer hardware or software or computing
10 devices with encryption capabilities covered
11 under this subsection; or

12 “(F) any encryption hardware or software
13 or computing device not used for confidentiality
14 purposes, such as authentication, integrity, elec-
15 tronic signatures, nonrepudiation, or copy pro-
16 tection.

17 “(3) COMPUTER HARDWARE OR SOFTWARE OR
18 COMPUTING DEVICES WITH ENCRYPTION CAPABILI-
19 TIES.—After a one-time, 15-day technical review by
20 the Secretary, the Secretary shall authorize the ex-
21 port or reexport of computer hardware or software
22 or computing devices with encryption capabilities for
23 nonmilitary end uses in any country—

24 “(A) to which exports of computer hard-
25 ware or software or computing devices of com-

1 parable strength are permitted for use by finan-
2 cial institutions not controlled in fact by United
3 States persons, unless there is substantial evi-
4 dence that such computer hardware or software
5 or computing devices will be—

6 “(i) diverted to a military end use or
7 an end use supporting international terror-
8 ism;

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

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

14 “(B) if the Secretary determines that a
15 computer hardware or software or computing
16 device offering comparable security is commer-
17 cially available outside the United States from
18 a foreign supplier, without effective restrictions.

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

21 “(A)(i) the term ‘encryption’ means the
22 scrambling of wire communications, electronic
23 communications, or electronically stored infor-
24 mation, using mathematical formulas or algo-
25 rithms in order to preserve the confidentiality,

1 integrity, or authenticity of, and prevent unau-
2 thorized recipients from accessing or altering,
3 such communications or information;

4 “(ii) the terms ‘wire communication’ and
5 ‘electronic communication’ have the meanings
6 given those terms in section 2510 of title 18,
7 United States Code;

8 “(B) the term ‘generally available’ means,
9 in the case of computer hardware or computer
10 software (including computer hardware or com-
11 puter software with encryption capabilities)—

12 “(i) computer hardware or computer
13 software that is—

14 “(I) distributed through the
15 Internet;

16 “(II) offered for sale, license, or
17 transfer to any person without restric-
18 tion, whether or not for consideration,
19 including, but not limited to, over-the-
20 counter retail sales, mail order trans-
21 actions, phone order transactions,
22 electronic distribution, or sale on ap-
23 proval;

24 “(III) preloaded on computer
25 hardware or computing devices that

1 are widely available for sale to the
2 public; or

3 “(IV) assembled from computer
4 hardware or computer software com-
5 ponents that are widely available for
6 sale to the public;

7 “(ii) not designed, developed, or tai-
8 lored by the manufacturer for specific pur-
9 chasers or users, except that any such pur-
10 chaser or user may—

11 “(I) supply certain installation
12 parameters needed by the computer
13 hardware or software to function
14 properly with the computer system of
15 the user or purchaser; or

16 “(II) select from among options
17 contained in the computer hardware
18 or computer software; and

19 “(iii) with respect to which the manu-
20 facturer of that computer hardware or
21 computer software—

22 “(I) intended for the user or pur-
23 chaser, including any licensee or
24 transferee, to install the computer
25 hardware or software and has sup-

1 plied the necessary instructions to do
2 so, except that the manufacturer of
3 the computer hardware or software, or
4 any agent of such manufacturer, may
5 also provide telephone or electronic
6 mail help line services for installation,
7 electronic transmission, or basic oper-
8 ations; and

9 “(II) the computer hardware or
10 software is designed for such installa-
11 tion by the user or purchaser without
12 further substantial support by the
13 manufacturer;

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

19 “(D) the term ‘computer hardware’ in-
20 cludes, but is not limited to, computer systems,
21 equipment, application-specific assemblies,
22 smart cards, modules, integrated circuits, and
23 printed circuit board assemblies;

24 “(E) the term ‘customer premises equip-
25 ment’ means equipment employed on the prem-

1 ises of a person to originate, route, or terminate
2 communications;

3 “(F) the term ‘technical assistance’ in-
4 cludes instruction, skills training, working
5 knowledge, consulting services, and the transfer
6 of technical data;

7 “(G) the term ‘technical data’ includes
8 blueprints, plans, diagrams, models, formulas,
9 tables, engineering designs and specifications,
10 and manuals and instructions written or re-
11 corded on other media or devices such as disks,
12 tapes, or read-only memories; and

13 “(H) the term ‘technical review’ means a
14 review by the Secretary of computer hardware
15 or software or computing devices with
16 encryption capabilities, based on information
17 about the product’s encryption capabilities sup-
18 plied by the manufacturer, that the computer
19 hardware or software or computing device
20 works as represented.”.

21 (b) NO REINSTATEMENT OF EXPORT CONTROLS ON
22 PREVIOUSLY DECONTROLLED PRODUCTS.—Any
23 encryption product not requiring an export license as of
24 the date of enactment of this Act, as a result of adminis-

1 trative decision or rulemaking, shall not require an export
2 license on or after such date of enactment.

3 (c) APPLICABILITY OF CERTAIN EXPORT CON-
4 TROLS.—

5 (1) IN GENERAL.—Nothing in this Act shall
6 limit the authority of the President under the Inter-
7 national Emergency Economic Powers Act, the
8 Trading with the enemy Act, or the Export Adminis-
9 tration Act of 1979, to—

10 (A) prohibit the export of encryption prod-
11 ucts to countries that have been determined to
12 repeatedly provide support for acts of inter-
13 national terrorism; or

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

16 (2) SPECIFIC DENIALS.—The Secretary may
17 prohibit the export of specific encryption products to
18 an individual or organization in a specific foreign
19 country identified by the Secretary, if the Secretary
20 determines that there is substantial evidence that
21 such encryption products will be used for military or
22 terrorist end-use.

23 (3) DEFINITION.—As used in this subsection
24 and subsection (b), the term “encryption” has the
25 meaning given that term in section 17(g)(5)(A) of

1 the Export Administration Act of 1979, as added by
2 subsection (a) of this section.

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

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

8 (a) COLLECTION OF INFORMATION BY ATTORNEY
9 GENERAL.—The Attorney General shall compile, and
10 maintain 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
13 the ability of the Department of Justice to enforce the
14 criminal 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.