

106TH CONGRESS
1ST SESSION

H. R. 2616

To clarify the policy of the United States with respect to the use and export of encryption products, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 27, 1999

Mr. GOSS (for himself, Mr. DIXON, Mr. LEWIS of California, Mr. CASTLE, Mr. BOEHLERT, Mr. BASS, Mr. GIBBONS, Mr. LAHOOD, Mrs. WILSON, Mr. BISHOP, Mr. SISISKY, Mr. CONDIT, Mr. HASTINGS of Florida, Mr. GILMAN, Mr. OXLEY, and Mr. STEARNS) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committees on International Relations, and Government Reform, 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

A BILL

To clarify the policy of the United States with respect to the use and export of encryption products, and for other purposes.

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

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

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

1 (b) TABLE OF CONTENTS.—The table of contents is
 2 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.

3 **SEC. 2. STATEMENT OF POLICY.**

4 It is the policy of the United States to protect public
 5 computer networks through the use of strong encryption

1 technology, to promote the export of encryption products
2 developed and manufactured in the United States, and to
3 preserve public safety and national security.

4 **SEC. 3. CONGRESSIONAL FINDINGS.**

5 The Congress finds the following:

6 (1) Information security technology, encryption,
7 is—

8 (A) fundamental to secure the flow of in-
9 telligence information to national policy makers;

10 (B) critical to the President and national
11 command authority of the United States;

12 (C) necessary to the Secretary of State for
13 the development and execution of the foreign
14 policy of the United States;

15 (D) essential to the Secretary of Defense's
16 responsibilities to ensure the effectiveness of the
17 Armed Forces of the United States;

18 (E) invaluable to the protection of the citi-
19 zens of the United States from fraud, theft,
20 drug trafficking, child pornography, kidnap-
21 ping, and money laundering; and

22 (F) basic to the protection of the nation's
23 critical infrastructures, including electrical
24 grids, banking and financial systems, tele-

1 communications, water supplies, and transpor-
2 tation.

3 (2) The goal of any encryption legislation
4 should be to enhance and promote the global market
5 strength of United States encryption manufacturers,
6 while guaranteeing that national security and public
7 safety obligations of the Government can still be ac-
8 complished.

9 (3) It is essential to the national security inter-
10 ests of the United States that United States
11 encryption products dominate the global market.

12 (4) Widespread use of unregulated encryption
13 products poses a significant threat to the national
14 security interests of the United States.

15 (5) Leaving the national security and public
16 safety responsibilities of the Government to the mar-
17 ketplace alone is not consistent with the obligations
18 of the Government to protect the public safety and
19 to defend the Nation.

20 (6) In order for the United States position in
21 the global market to benefit the national security in-
22 terests of the United States, it is imperative that the
23 export of encryption products be subject to a dy-
24 namic and constructive export control regime.

1 (7) Export of commercial items are best man-
2 aged through a regulatory structure which has flexi-
3 bility to address constantly changing market condi-
4 tions.

5 (8) Managing sensitive dual-use technologies,
6 such as encryption products, is challenging in any
7 regulatory environment due to the difficulty in bal-
8 ancing competing interests in national security, pub-
9 lic safety, privacy, fair competition within the indus-
10 try, and the dynamic nature of the technology.

11 (9) There is a widespread perception that the
12 executive branch has not adequately balanced the
13 equal and competing interests of national security,
14 public safety, privacy, and industry.

15 (10) There is a perception that the current
16 encryption export control policy has done more to
17 disadvantage United States business interests than
18 to promote and protect national security and public
19 safety interests.

20 (11) A balance can and must be achieved be-
21 tween industry interests, national security, law en-
22 forcement requirements, and privacy needs.

23 (12) A court order process should be required
24 for access to plaintext, where and when available,

1 and criminal and civil penalties should be imposed
2 for misuse of decryption information.

3 (13) Timely access to plaintext capability is—

4 (A) necessary to thwarting potential ter-
5 rorist activities;

6 (B) extremely useful in the collection of
7 foreign intelligence;

8 (C) indispensable to force protection re-
9 quirements;

10 (D) critical to the investigation and pros-
11 ecution of criminals; and

12 (E) both technically and economically pos-
13 sible.

14 (14) The United States Government should en-
15 courage the development of those products that
16 would provide a capability allowing law enforcement
17 (Federal, State, and local), with a court order only,
18 to gain timely access to the plaintext of either stored
19 data or data in transit.

20 (15) Unless law enforcement has the benefit of
21 such market encouragement, drug traffickers, spies,
22 child pornographers, pedophiles, kidnappers, terror-
23 ists, mobsters, weapons proliferators, fraud schem-
24 ers, and other criminals will be able to use

1 encryption software to protect their criminal activity
2 and hinder the criminal justice system.

3 (16) An effective regulatory approach to man-
4 age the proliferation of encryption products which
5 have dual-use capabilities must be maintained and
6 greater confidence in the ability of the executive
7 branch to preserve and promote the competitive ad-
8 vantage of the United States encryption industry in
9 the global market must be provided.

10 **TITLE I—DOMESTIC USES OF** 11 **ENCRYPTION**

12 **SEC. 101. DEFINITIONS.**

13 For purposes of this Act:

14 (1) **ATTORNEY FOR THE GOVERNMENT.**—The
15 term “attorney for the Government” has the mean-
16 ing given such term in Rule 54(e) of the Federal
17 Rules of Criminal Procedure, and also includes any
18 duly authorized attorney of a State who is author-
19 ized to prosecute criminal offenses within such
20 State.

21 (2) **AUTHORIZED PARTY.**—The term “author-
22 ized party” means any person with the legal author-
23 ity to obtain decryption information or plaintext of
24 encrypted data, including communications.

1 (3) COMMUNICATIONS.—The term “communica-
2 tions” means any wire communications or electronic
3 communications as those terms are defined in para-
4 graphs (1) and (12) of section 2510 of title 18,
5 United States Code.

6 (4) COURT OF COMPETENT JURISDICTION.—
7 The term “court of competent jurisdiction” means
8 any court of the United States organized under Arti-
9 cle III of the Constitution of the United States, the
10 court organized under the Foreign Intelligence Sur-
11 veillance Act of 1978 (50 U.S.C. 1801 et seq.), or
12 a court of general criminal jurisdiction of a State
13 authorized pursuant to the laws of such State to
14 enter orders authorizing searches and seizures.

15 (5) DATA NETWORK SERVICE PROVIDER.—The
16 term “data network service provider” means a per-
17 son offering any service to the general public that
18 provides the users thereof with the ability to trans-
19 mit or receive data, including communications.

20 (6) DECRYPTION.—The term “decryption”
21 means the retransformation or unscrambling of
22 encrypted data, including communications, to its
23 readable plaintext version. To “decrypt” data, in-
24 cluding communications, is to perform decryption.

1 (7) DECRYPTION INFORMATION.—The term
2 “decryption information” means information or tech-
3 nology that enables one to readily retransform or
4 unscramble encrypted data from its unreadable and
5 incomprehensible format to its readable plaintext
6 version.

7 (8) ELECTRONIC STORAGE.—The term “elec-
8 tronic storage” has the meaning given that term in
9 section 2510(17) of title 18, United States Code.

10 (9) ENCRYPTION.—The term “encryption”
11 means the transformation or scrambling of data, in-
12 cluding communications, from plaintext to an
13 unreadable or incomprehensible format, regardless of
14 the technique utilized for such transformation or
15 scrambling and irrespective of the medium in which
16 such data, including communications, occur or can
17 be found, for the purposes of protecting the content
18 of such data, including communications. To
19 “encrypt” data, including communications, is to per-
20 form encryption.

21 (10) ENCRYPTION PRODUCT.—The term
22 “encryption product” means any software, tech-
23 nology, commodity, or mechanism, that can be used
24 to encrypt or decrypt or has the capability of

1 encrypting or decrypting any data, including commu-
2 nications.

3 (11) FOREIGN AVAILABILITY.—The term “for-
4 eign availability” has the meaning applied to foreign
5 availability of encryption products subject to controls
6 under the Export Administration Regulations, as in
7 effect on July 1, 1999.

8 (12) GOVERNMENT.—The term “Government”
9 means the Government of the United States and any
10 agency or instrumentality thereof, or the government
11 of any State, and any of its political subdivisions.

12 (13) INVESTIGATIVE OR LAW ENFORCEMENT
13 OFFICER.—The term “investigative or law enforce-
14 ment officer” has the meaning given that term in
15 section 2510(7) of title 18, United States Code.

16 (14) NATIONAL SECURITY.—The term “na-
17 tional security” means the national defense, intel-
18 ligence, or foreign policy interests of the United
19 States.

20 (15) PLAINTEXT.—The term “plaintext” means
21 the readable or comprehensible format of that data,
22 including communications, which has been
23 encrypted.

24 (16) PLAINVOICE.—The term “plainvoice”
25 means communication specific plaintext.

1 (17) SECRETARY.—The term “Secretary”
2 means the Secretary of Commerce, unless otherwise
3 specifically identified.

4 (18) STATE.—The term “State” has the mean-
5 ing given that term in section 2510(3) of title 18,
6 United States Code.

7 (19) TELECOMMUNICATIONS CARRIER.—The
8 term “telecommunications carrier” has the meaning
9 given that term in section 3 of the Communications
10 Act of 1934 (47 U.S.C. 153).

11 (20) TELECOMMUNICATIONS SYSTEM.—The
12 term “telecommunications system” means any
13 equipment, technology, or related software used in
14 the movement, switching, interchange, transmission,
15 reception, or internal signaling of data, including
16 communications over wire, fiber optic, radio fre-
17 quency, or any other medium.

18 (21) UNITED STATES PERSON.—The term
19 “United States person” means—

20 (A) any citizen of the United States;

21 (B) any other person organized under the
22 laws of any State; and

23 (C) any person organized under the laws of
24 any foreign country who is owned or controlled

1 by individuals or persons described in subpara-
2 graphs (A) and (B).

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

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

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

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

14 **“CHAPTER 125—ENCRYPTED DATA,**
15 **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.

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

18 “(a) PROHIBITED ACTS.—Whoever knowingly uses
19 encryption in furtherance of the commission of a criminal
20 offense for which the person may be prosecuted in a dis-
21 trict court of the United States shall—

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

4 “(2) in the case of a second or subsequent of-
5 fense under this section, be imprisoned for not more
6 than 10 years, or fined under this title, or both.

7 “(b) CONSECUTIVE SENTENCE.—Notwithstanding
8 any other provision of law, the court shall not place on
9 probation any person convicted of a violation of this sec-
10 tion, nor shall the term of imprisonment imposed under
11 this section run concurrently with any other term of im-
12 prisonment imposed for the underlying criminal offense.

13 “(c) PROBABLE CAUSE NOT CONSTITUTED BY USE
14 OF ENCRYPTION.—The use of encryption by itself shall
15 not establish probable cause to believe that a crime is
16 being or has been committed.

17 **“§ 2802. Privacy protection**

18 “(a) IN GENERAL.—It shall be unlawful for any per-
19 son to intentionally—

20 “(1) obtain or use decryption information with-
21 out lawful authority for the purpose of decrypting
22 data, including communications;

23 “(2) exceed lawful authority in decrypting data,
24 including communications;

1 “(A) upon the application by an attorney for
2 the Government that—

3 “(i) is made under oath or affirmation by
4 the attorney for the Government; and

5 “(ii) provides a factual basis establishing
6 the relevance that the plaintext or decryption
7 information being sought has to a law enforce-
8 ment, foreign counterintelligence, or inter-
9 national terrorism investigation then being con-
10 ducted pursuant to lawful authorities; and

11 “(B) if the court finds, in writing, that the
12 plaintext or decryption information being sought is
13 relevant to an ongoing lawful law enforcement, for-
14 eign counterintelligence, or international terrorism
15 investigation and the investigative or law enforce-
16 ment officer is entitled to such plaintext or
17 decryption information.

18 “(2) The order issued by the court under this section
19 shall be placed under seal, except that a copy may be made
20 available to the investigative or law enforcement officer
21 authorized to obtain access to the plaintext of the
22 encrypted information, or authorized to obtain the
23 decryption information sought in the application. Such
24 order shall, subject to the notification procedures set forth
25 in section 2804, also be made available to the person re-

1 sponsible for providing the plaintext or the decryption in-
2 formation, pursuant to such order, to the investigative or
3 law enforcement officer.

4 “(3) Disclosure of an application made, or order
5 issued, under this section, is not authorized, except as may
6 otherwise be specifically permitted by this section or an-
7 other order of the court.

8 “(b) RECORD OF ACCESS REQUIRED.—(1) There
9 shall be created an electronic record, or similar type
10 record, of each instance in which an investigative or law
11 enforcement officer, pursuant to an order under this sec-
12 tion, gains access to the plaintext of otherwise encrypted
13 information, or is provided decryption information, with-
14 out the knowledge or consent of the owner of the data,
15 including communications, who is the user of the
16 encryption product involved.

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

24 “(3) The court receiving such electronic or similar
25 type of record described in paragraph (1) shall make the

1 original and a certified copy of the record available to the
2 attorney for the Government making application under
3 this section, and to the attorney for, or directly to, the
4 owner of the data, including communications, who is the
5 user of the encryption product, pursuant to the notifica-
6 tion procedures set forth in section 2804.

7 “(c) AUTHORITY TO INTERCEPT COMMUNICATIONS
8 NOT INCREASED.—Nothing in this chapter shall be con-
9 strued to enlarge or modify the circumstances or proce-
10 dures under which a Government entity is entitled to
11 intercept or obtain oral, wire, or electronic communica-
12 tions or information.

13 “(d) CONSTRUCTION.—This chapter shall be strictly
14 construed to apply only to a Government entity’s ability
15 to decrypt data, including communications, for which it
16 has previously obtained lawful authority to intercept or ob-
17 tain pursuant to other lawful authorities, which without
18 an order issued under this section would otherwise remain
19 encrypted.

20 **“§ 2804. Notification procedures**

21 “(a) IN GENERAL.—Within a reasonable time, but
22 not later than 90 days after the filing of an application
23 for an order under section 2803 which is granted, the
24 court shall cause to be served, on the persons named in
25 the order or the application, and such other parties whose

1 decryption information or whose plaintext has been pro-
2 vided to an investigative or law enforcement officer pursu-
3 ant to this chapter, as the court may determine is in the
4 interest of justice, an inventory which shall include notice
5 of—

6 “(1) the fact of the entry of the order or the
7 application;

8 “(2) the date of the entry of the application
9 and issuance of the order; and

10 “(3) the fact that the person’s decryption infor-
11 mation or plaintext data, including communications,
12 has been provided or accessed by an investigative or
13 law enforcement officer.

14 The court, upon the filing of a motion, may make available
15 to that person or that person’s counsel, for inspection,
16 such portions of the plaintext, applications, and orders as
17 the court determines to be in the interest of justice.

18 “(b) POSTPONEMENT OF INVENTORY FOR GOOD
19 CAUSE.—(1) On an ex parte showing of good cause by
20 an attorney for the Government to a court of competent
21 jurisdiction, the serving of the inventory required by sub-
22 section (a) may be postponed for an additional 30 days
23 after the granting of an order pursuant to the ex parte
24 motion.

1 “(2) No more than 3 ex parte motions pursuant to
2 paragraph (1) are authorized.

3 “(c) ADMISSION INTO EVIDENCE.—The content of
4 any encrypted information that has been obtained pursu-
5 ant to this chapter or evidence derived therefrom shall not
6 be received in evidence or otherwise disclosed in any trial,
7 hearing, or other proceeding in a Federal or State court,
8 other than the court organized pursuant to the Foreign
9 Intelligence Surveillance Act of 1978, unless each party,
10 not less than 10 days before the trial, hearing, or pro-
11 ceeding, has been furnished with a copy of the order, and
12 accompanying application, under which the decryption or
13 access to plaintext was authorized or approved. This 10-
14 day period may be waived by the court if the court finds
15 that it was not possible to furnish the party with the infor-
16 mation described in the preceding sentence within 10 days
17 before the trial, hearing, or proceeding and that the party
18 will not be prejudiced by the delay in receiving such infor-
19 mation.

20 “(d) CONSTRUCTION.—The provisions of this chapter
21 shall be construed consistent with—

22 “(1) the Classified Information Procedures Act
23 (18 U.S.C. App.); and

24 “(2) the Foreign Intelligence Surveillance Act
25 of 1978 (50 U.S.C. 1801 et seq.).

1 “(e) CONTEMPT.—Any violation of the provisions of
2 this section may be punished by the court as a contempt
3 thereof.

4 “(f) MOTION TO SUPPRESS.—Any aggrieved person
5 in any trial, hearing, or proceeding in or before any court,
6 department, officer, agency, regulatory body, or other au-
7 thority of the United States or a State, other than the
8 court organized pursuant to the Foreign Intelligence Sur-
9 veillance Act of 1978, may move to suppress the contents
10 of any decrypted data, including communications, ob-
11 tained pursuant to this chapter, or evidence derived there-
12 from, on the grounds that—

13 “(1) the plaintext was decrypted or accessed in
14 violation of this chapter;

15 “(2) the order of authorization or approval
16 under which it was decrypted or accessed is insuffi-
17 cient on its face; or

18 “(3) the decryption was not made in conformity
19 with the order of authorization or approval.

20 Such motion shall be made before the trial, hearing, or
21 proceeding unless there was no opportunity to make such
22 motion, or the person was not aware of the grounds of
23 the motion. If the motion is granted, the plaintext of the
24 decrypted data, including communications, or evidence de-
25 rived therefrom, shall be treated as having been obtained

1 in violation of this chapter. The court, upon the filing of
2 such motion by the aggrieved person, may make available
3 to the aggrieved person or that person’s counsel for in-
4 spection such portions of the decrypted plaintext, or evi-
5 dence derived therefrom, as the court determines to be in
6 the interests of justice.

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

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

24 “(i) COVERED PERSONS.—Subsection (h) applies to
25 any person whose decryption information—

1 “(1) is knowingly obtained without lawful au-
2 thority by an investigative or law enforcement offi-
3 cer;

4 “(2) is obtained by an investigative or law en-
5 forcement officer with lawful authority and is know-
6 ingly used or disclosed by such officer unlawfully; or

7 “(3) is obtained by an investigative or law en-
8 forcement officer with lawful authority and whose
9 decryption information is unlawfully used to disclose
10 the plaintext of the data, including communications.

11 “(j) LIMITATION.—A civil action under subsection (h)
12 shall be commenced not later than 2 years after the date
13 on which the unlawful action took place, or 2 years after
14 the date on which the claimant first discovers the viola-
15 tion, whichever is later.

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

23 “(l) TECHNICAL ASSISTANCE BY PROVIDERS.—A
24 provider of encryption technology or network service that
25 has received an order issued by a court pursuant to this

1 chapter shall provide to the investigative or law enforce-
2 ment officer concerned such technical assistance as is nec-
3 essary to execute the order. Such provider may, however,
4 move the court to modify or quash the order on the ground
5 that its assistance with respect to the decryption or access
6 to plaintext cannot be performed in fact, or in a timely
7 or reasonable fashion. The court, upon notice to the Gov-
8 ernment, shall decide such motion expeditiously.

9 “(m) REPORTS TO CONGRESS.—In May of each year,
10 the Attorney General, or an Assistant Attorney General
11 specifically designated by the Attorney General, shall re-
12 port in writing to Congress on the number of applications
13 made and orders entered authorizing Federal, State, and
14 local law enforcement access to decryption information for
15 the purposes of reading the plaintext of otherwise
16 encrypted data, including communications, pursuant to
17 this chapter. Such reports shall be submitted to the Com-
18 mittees on the Judiciary of the House of Representatives
19 and of the Senate, and to the Permanent Select Com-
20 mittee on Intelligence for the House of Representatives
21 and the Select Committee on Intelligence for the Senate.

22 **“§ 2805. Lawful use of plaintext or decryption infor-**
23 **mation**

24 “(a) AUTHORIZED USE OF DECRYPTION INFORMA-
25 TION.—

1 “(1) CRIMINAL INVESTIGATIONS.—An inves-
2 tigative or law enforcement officer to whom plaintext
3 or decryption information is provided may only use
4 such plaintext or decryption information for the pur-
5 poses of conducting a lawful criminal investigation,
6 foreign counterintelligence, or international ter-
7 rorism investigation, and for the purposes of pre-
8 paring for and prosecuting any criminal violation of
9 law.

10 “(2) CIVIL REDRESS.—Any plaintext or
11 decryption information provided under this chapter
12 to an investigative or law enforcement officer may
13 not be disclosed, except by court order, to any other
14 person for use in a civil proceeding that is unrelated
15 to a criminal investigation and prosecution for which
16 the plaintext or decryption information is authorized
17 under paragraph (1). Such order shall only issue
18 upon a showing by the party seeking disclosure that
19 there is no alternative means of obtaining the
20 plaintext, or decryption information, being sought
21 and the court also finds that the interests of justice
22 would not be served by nondisclosure.

23 “(b) LIMITATION.—An investigative or law enforce-
24 ment officer may not use decryption information obtained
25 under this chapter to determine the plaintext of any data,

1 including communications, unless it has obtained lawful
2 authority to obtain such data, including communications,
3 under other lawful authorities.

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

7 “(1)(A) return any decryption information to
8 the person responsible for providing it to an inves-
9 tigative or law enforcement officer pursuant to this
10 chapter; or

11 “(B) destroy such decryption information, if the
12 court finds that the interests of justice or public
13 safety require that such decryption information
14 should not be returned to the provider; and

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

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

22 “(B) if applicable, notify the provider of
23 the decryption information of the destruction of
24 such information.

1 “(d) OTHER DISCLOSURE OF DECRYPTION INFORMA-
2 TION.—Except as otherwise provided in section 2803,
3 decryption information or the plaintext of otherwise
4 encrypted data, including communications, shall not be
5 disclosed by any person unless the disclosure is—

6 “(1) to the person encrypting the data, includ-
7 ing communications, or an authorized agent thereof;

8 “(2) with the consent of the person encrypting
9 the data, including pursuant to a contract entered
10 into with the person;

11 “(3) pursuant to a court order upon a showing
12 of compelling need for the information that cannot
13 be accommodated by any other means if—

14 “(A) the person who supplied the informa-
15 tion is given reasonable notice, by the person
16 seeking the disclosure, of the court proceeding
17 relevant to the issuance of the court order; and

18 “(B) the person who supplied the informa-
19 tion is afforded the opportunity to appear in the
20 court proceeding and contest the claim of the
21 person seeking the disclosure;

22 “(4) pursuant to a determination by a court of
23 competent jurisdiction that another person is law-
24 fully entitled to hold such decryption information,
25 including determinations arising from legal pro-

1 proceedings associated with the incapacity, death, or
 2 dissolution of any person; or

3 “(5) otherwise permitted by law.

4 **“§ 2806. Identification of decryption information**

5 “(a) IDENTIFICATION.—To avoid inadvertent disclo-
 6 sure of decryption information, any person who provides
 7 decryption information to an investigative or law enforce-
 8 ment officer pursuant to this chapter shall specifically
 9 identify that part of the material that discloses decryption
 10 information as such.

11 “(b) RESPONSIBILITY OF INVESTIGATIVE OR LAW
 12 ENFORCEMENT OFFICER.—The investigative or law en-
 13 forcement officer receiving any decryption information
 14 under this chapter shall maintain such information in a
 15 facility and in a method so as to reasonably assure that
 16 inadvertent disclosure does not occur.

17 **“§ 2807. Definitions**

18 “The definitions set forth in section 101 of the
 19 Encryption for the National Interest Act shall apply to
 20 this chapter.”.

21 (b) CONFORMING AMENDMENT.—The table of chap-
 22 ters for part I of title 18, United States Code, is amended
 23 by inserting after the item relating to chapter 121 the fol-
 24 lowing new item:

“125. Encrypted data, including communications 2801”.

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

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

5 (a) **DECRYPTION CAPABILITIES.**—The President
6 may, consistent with the provisions of subsection (b), di-
7 rect that any encryption product or service purchased or
8 otherwise procured by the United States Government to
9 provide the security service of data confidentiality for a
10 computer system owned and operated by the United States
11 Government shall include recoverability features or func-
12 tions that enable the timely decryption of encrypted data,
13 including communications, or timely access to plaintext by
14 an authorized party without the knowledge or cooperation
15 of the person using such encryption products or services.

16 (b) **CONSISTENCY WITH INTELLIGENCE SERVICES**
17 **AND MILITARY OPERATIONS.**—The President shall ensure
18 that all encryption products purchased or used by the
19 United States Government are supportive of, and con-
20 sistent with, all statutory obligations to protect sources
21 and methods of intelligence collection and activities, and
22 supportive of, and consistent with, those needs required
23 for military operations and the conduct of foreign policy.

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

2 The President may direct that any communications
3 network established for the purpose of conducting the
4 business of the Federal Government shall use encryption
5 products that—

6 (1) include features and functions that enable
7 the timely decryption of encrypted data, including
8 communications, or timely access to plaintext, by an
9 authorized party without the knowledge or coopera-
10 tion of the person using such encryption products or
11 services; and

12 (2) are supportive of, and consistent with, all
13 statutory obligations to protect sources and methods
14 of intelligence collection and activities, and sup-
15 portive of, and consistent with, those needs required
16 for military operations and the conduct of foreign
17 policy.

18 **SEC. 203. GOVERNMENT CONTRACT AUTHORITY.**

19 The President may require as a condition of any con-
20 tract by the Government with a private sector vendor that
21 any encryption product used by the vendor in carrying out
22 the provisions of the contract with the Government include
23 features and functions that enable the timely decryption
24 of encrypted data, including communications, or timely ac-
25 cess to plaintext, by an authorized party without the

1 knowledge or cooperation of the person using such
2 encryption products or services.

3 **SEC. 204. PRODUCT LABELS.**

4 An encryption product may be labeled to inform Gov-
5 ernment users that the product is authorized for sale to
6 or for use by Government agencies or Government con-
7 tractors in transactions and communications with the
8 United States Government under this title.

9 **SEC. 205. NO PRIVATE MANDATE.**

10 The United States Government may not require the
11 use of encryption standards for the private sector except
12 as otherwise authorized by section 204.

13 **SEC. 206. EXCLUSION.**

14 Nothing in this title shall apply to encryption prod-
15 ucts and services used solely for access control, authentica-
16 tion, integrity, nonrepudiation, digital signatures, or other
17 similar purposes.

18 **TITLE III—EXPORTS OF**
19 **ENCRYPTION**

20 **SEC. 301. EXPORTS OF ENCRYPTION.**

21 (a) **AUTHORITY TO CONTROL EXPORTS.**—The Presi-
22 dent shall control the export of all dual-use encryption
23 products.

24 (b) **AUTHORITY TO DENY EXPORT FOR NATIONAL**
25 **SECURITY REASONS.**—Notwithstanding any provision of

1 this title, the President may deny the export of any
2 encryption product on the basis that its export is contrary
3 to the national security.

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

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

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

14 (1) such encryption product is submitted for a
15 1-time technical review;

16 (2) such encryption product does not require li-
17 censing under otherwise applicable regulations;

18 (3) such encryption product is not intended for
19 a country, end user, or end use that is by regulation
20 ineligible to receive such product, and the encryption
21 product is otherwise qualified for export;

22 (4) the exporter, within 180 days after the ex-
23 port of the product, submits a certification
24 identifying—

1 (A) the intended end use of the product;
2 and

3 (B) the name and address of the intended
4 recipient of the product, where available;

5 (5) the exporter, within 180 days of the export
6 of the product, provides the names and addresses of
7 its distribution chain partners; and

8 (6) the exporter, at the time of submission of
9 the product for technical review, provides proof that
10 its distribution chain partners have contractually
11 agreed to abide by all laws and regulations of the
12 United States concerning the export and reexport of
13 encryption products designed or manufactured with-
14 in the United States.

15 (b) ONE-TIME TECHNICAL REVIEW.—(1) The tech-
16 nical review referred to in subsection (a) shall be com-
17 pleted within no longer than 45 days after the submission
18 of all of the information required under paragraph (2).

19 (2) The President shall specify the information that
20 must be submitted for the 1-time technical review referred
21 to in this section.

22 (3) An encryption product may not be exported dur-
23 ing the technical review of that product under this section.

24 (c) PERIODIC REVIEW OF LICENSE EXCEPTION ELI-
25 GIBILITY LEVEL.—(1) Not later than 180 days after the

1 date of the enactment of this Act, the President shall no-
2 tify the Congress of the maximum level of encryption
3 strength, which may not be lower than 64-bit, that may
4 be exported from the United States under license excep-
5 tion pursuant to this section consistent with the national
6 security.

7 (2) The President shall, at the end of each successive
8 180-day period after the notice provided to the Congress
9 under paragraph (1), notify the Congress of the maximum
10 level of encryption strength, which may not be lower than
11 that in effect under this section during that 180-day pe-
12 riod, that may be exported from the United States under
13 a license exception pursuant to this section consistent with
14 the national security.

15 (d) **FACTORS NOT TO BE CONSIDERED.**—A license
16 exception for the exports of an encryption product under
17 this section may be allowed whether or not the product
18 contains a method of decrypting encrypted data.

19 **SEC. 303. DISCRETIONARY AUTHORITY.**

20 Notwithstanding the requirements of section 305, the
21 President may permit the export, under a license exception
22 pursuant to the conditions of section 302, of encryption
23 products with an encryption strength exceeding the max-
24 imum level eligible for a license exception under section
25 302, if the export is consistent with the national security.

1 **SEC. 304. EXPEDITED REVIEW AUTHORITY.**

2 The President shall establish procedures for the expe-
3 dited review of commodity classification requests, or ex-
4 port license applications, involving encryption products
5 that are specifically approved, by regulation, for export.

6 **SEC. 305. ENCRYPTION LICENSES REQUIRED.**

7 (a) UNITED STATES PRODUCTS EXCEEDING CER-
8 TAIN BIT LENGTH.—Except as permitted under section
9 303, in the case of all encryption products with an
10 encryption strength exceeding the maximum level eligible
11 for a license exception under section 302, which are de-
12 signed or manufactured within the United States, the
13 President may grant a license for export of such
14 encryption products, under the following conditions:

15 (1) There shall not be any requirement, as a
16 basis for an export license, that a product contains
17 a method of—

18 (A) gaining timely access to plaintext; or

19 (B) gaining timely access to decryption in-
20 formation.

21 (2) The export license applicant shall submit—

22 (A) the product for technical review;

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

25 (i) the intended end use of the prod-
26 uct; and

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

3 (C) proof that its distribution chain part-
4 ners have contractually agreed to abide by all
5 laws and regulations of the United States con-
6 cerning the export and reexport of encryption
7 products designed or manufactured within the
8 United States; and

9 (D) the names and addresses of its dis-
10 tribution chain partners.

11 (b) TECHNICAL REVIEW FOR LICENSE APPLI-
12 CANTS.—(1) The technical review described in subsection
13 (a)(3)(A) shall be completed within 45 days after the sub-
14 mission of all the information required under paragraph
15 (2).

16 (2) The information to be submitted for the technical
17 review shall be the same as that required to be submitted
18 pursuant to section 302(b)(2).

19 (3) An encryption product may not be exported dur-
20 ing the technical review of that product under this section.

21 (c) POST-EXPORT REPORTING.—

22 (1) UNAUTHORIZED USE.—All exporters of
23 encryption products that are designed or manufac-
24 tured within the United States shall submit a report
25 to the Secretary at any time the exporter has reason

1 to believe any such exported product is being di-
2 verted to a use or a user not approved at the time
3 of export.

4 (2) PIRATING.—All exporters of encryption
5 products that are designed or manufactured within
6 the United States shall report any pirating of their
7 technology or intellectual property to the Secretary
8 as soon as practicable after discovery.

9 (3) DISTRIBUTION CHAIN PARTNERS.—All ex-
10 porters of encryption products that are designed or
11 manufactured within the United States, and all dis-
12 tribution chain partners of such exporters, shall sub-
13 mit to the Secretary a report which shall specify—

14 (A) the particular product sold;

15 (B) the name and address of—

16 (i) the ultimate end user of the prod-
17 uct, if known; or

18 (ii) the name and address of the next
19 purchaser in the distribution chain; and

20 (C) the intended use of the product sold.

21 (d) EXERCISE OF OTHER AUTHORITIES.—The Sec-
22 retary, the Secretary of Defense, and the Secretary of
23 State may exercise the authorities they have under other
24 provisions of law, including the Export Administration Act

1 of 1979, as continued in effect under the International
2 Emergency Economic Powers Act, to carry out this title.

3 (e) WAIVER AUTHORITY.—

4 (1) IN GENERAL.—The President may by Exec-
5 utive order waive any provision of this title, or the
6 applicability of any such provision to a person or en-
7 tity, if the President determines that the waiver is
8 necessary to advance the national security. The
9 President shall, not later than 15 days after making
10 such determination, submit a report to the commit-
11 tees referred to in paragraph (2) that includes the
12 factual basis upon which such determination was
13 made. The report may be in classified format.

14 (2) COMMITTEES.—The committees referred to
15 in paragraph (1) are the Committee on International
16 Relations, the Committee on Armed Services, and
17 the Permanent Select Committee on Intelligence of
18 the House of Representatives, and the Committee on
19 Foreign Relations, the Committee on Armed Serv-
20 ices, and the Select Committee on Intelligence of the
21 Senate.

22 (3) DECISIONS NOT SUBJECT TO JUDICIAL RE-
23 VIEW.—Any determination made by the President
24 under this subsection shall not be subject to judicial
25 review.

1 **SEC. 306. ENCRYPTION INDUSTRY AND INFORMATION SE-**
2 **CURITY BOARD.**

3 (a) ENCRYPTION INDUSTRY AND INFORMATION SE-
4 CURITY BOARD ESTABLISHED.—There is hereby estab-
5 lished an Encryption Industry and Information Security
6 Board. The Board shall undertake an advisory role for the
7 President.

8 (b) PURPOSES.—The purposes of the Board are—

9 (1) to provide a forum to foster communication
10 and coordination between industry and the Federal
11 Government on matters relating to the use of
12 encryption products;

13 (2) to enable the United States to effectively
14 and continually understand the benefits and risks to
15 its national security, law enforcement, and public
16 safety interests by virtue of the proliferation of
17 strong encryption on the global market;

18 (3) to evaluate and make recommendations re-
19 garding the further development and use of
20 encryption;

21 (4) to advance the development of international
22 standards regarding interoperability and global use
23 of encryption products;

24 (5) to promote the export of encryption prod-
25 ucts manufactured in the United States;

1 (6) to recommend policies enhancing the secu-
2 rity of public networks;

3 (7) to encourage research and development of
4 products that will foster electronic commerce;

5 (8) to promote the protection of intellectual
6 property and privacy rights of individuals using pub-
7 lic networks; and

8 (9) to evaluate the availability and market
9 share of foreign encryption products and their threat
10 to United States industry.

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

13 (A) The Secretary, or the Secretary’s designee.

14 (B) The Attorney General, or his or her des-
15 ignee.

16 (C) The Secretary of Defense, or the Sec-
17 retary’s designee.

18 (D) The Director of Central Intelligence, or his
19 or her designee.

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

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

1 (G) Six representatives from the private sector
2 who have expertise in the development, operation,
3 marketing, law, or public policy relating to informa-
4 tion security or technology. Members under this sub-
5 paragraph shall each serve for 5-year terms.

6 (2) The six private sector representatives described
7 in paragraph (1)(G) shall be appointed as follows:

8 (A) Two by the Speaker of the House of
9 Representatives.

10 (B) One by the Minority Leader of the
11 House of Representatives.

12 (C) Two by the Majority Leader of the
13 Senate.

14 (D) One by the Minority Leader of the
15 Senate.

16 (e) MEETINGS.—The Board shall meet at such times
17 and in such places as the Secretary may prescribe, but
18 not less frequently than every four months. The Federal
19 Advisory Committee Act (5 U.S.C. App.) does not apply
20 to the Board or to meetings held by the Board under this
21 section.

22 (f) FINDINGS AND RECOMMENDATIONS.—The chair
23 of the Board shall convey the findings and recommenda-
24 tions of the Board to the President and to the Congress
25 within 30 days after each meeting of the Board. The rec-

1 ommendations of the Board are not binding upon the
2 President.

3 (g) LIMITATION.—The Board shall have no authority
4 to review any export determination made pursuant to this
5 title.

6 (h) FOREIGN AVAILABILITY.—The consideration of
7 foreign availability by the Board shall include computer
8 software that is distributed over the Internet or advertised
9 for sale, license, or transfer, including over-the-counter re-
10 tail sales, mail order transactions, telephone order trans-
11 actions, electronic distribution, or sale on approval and its
12 comparability with United States products and its use in
13 United States and foreign markets.

14 (i) TERMINATION.—This section shall cease to be ef-
15 fective 10 years after the date of the enactment of this
16 Act.

17 **TITLE IV—LIABILITY** 18 **LIMITATIONS**

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

20 (a) NO LIABILITY FOR COMPLIANCE.—Subject to
21 subsection (b), no civil or criminal liability under this Act,
22 or under any other provision of law, shall attach to any
23 person for disclosing or providing—

24 (1) the plaintext of encrypted data, including
25 communications;

1 (2) the decryption information of such
2 encrypted data, including communications; or

3 (3) technical assistance for access to the
4 plaintext of, or decryption information for, encrypted
5 data, including communications.

6 (b) EXCEPTION.—Subsection (a) shall not apply to
7 a person who provides plaintext or decryption information
8 to another in violation of the provisions of this Act.

9 **SEC. 402. COMPLIANCE DEFENSE.**

10 Compliance with the provisions of sections 2803,
11 2804, 2805, or 2806 of title 18, United States Code, as
12 added by section 103(a) of this Act, or any regulations
13 authorized by this Act, shall provide a complete defense
14 for any civil action for damages based upon activities cov-
15 ered by this Act, other than an action founded on contract.

16 **SEC. 403. GOOD FAITH DEFENSE.**

17 An objectively reasonable reliance on the legal author-
18 ity provided by this Act and the amendments made by this
19 Act, authorizing access to the plaintext of otherwise
20 encrypted data, including communications, or to
21 decryption information that will allow the timely
22 decryption of data, including communications, that is oth-
23 erwise encrypted, shall be an affirmative defense to any
24 criminal or civil action that may be brought under the laws
25 of the United States or any State.

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

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

4 It is the sense of Congress that—

5 (1) the President should conduct negotiations
6 with foreign governments for the purposes of estab-
7 lishing binding export control requirements on
8 strong nonrecoverable encryption products; and

9 (2) such agreements should safeguard the pri-
10 vacy of the citizens of the United States, prevent
11 economic espionage, and enhance the information se-
12 curity needs of the United States.

13 **SEC. 502. FAILURE TO NEGOTIATE.**

14 The President may consider a government’s refusal
15 to negotiate agreements described in section 501 when
16 considering the participation of the United States in any
17 cooperation or assistance program with that country.

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

19 (a) **REPORT TO CONGRESS.**—The President shall re-
20 port annually to the Congress on the status of the inter-
21 national effort outlined by section 501.

22 (b) **FIRST REPORT.**—The first report required under
23 subsection (a) shall be submitted in unclassified form no
24 later than September 1, 2000.

1 **TITLE VI—MISCELLANEOUS**
2 **PROVISIONS**

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

4 (a) **COLLECTION OF INFORMATION BY ATTORNEY**
5 **GENERAL.**—The Attorney General shall compile, and
6 maintain in classified form, data on—

7 (1) the instances in which encryption has inter-
8 ferred with, impeded, or obstructed the ability of the
9 Department of Justice to enforce the laws of the
10 United States; and

11 (2) the instances where the Department of Jus-
12 tice has been successful in overcoming any
13 encryption encountered in an investigation.

14 (b) **AVAILABILITY OF INFORMATION TO THE CON-**
15 **GRESS.**—The information compiled under subsection (a),
16 including an unclassified summary thereof, shall be sub-
17 mitted to Congress annually beginning October 1, 2000.

18 **SEC. 602. INTERPRETATION.**

19 Nothing contained in this Act or the amendments
20 made by this Act shall be deemed to—

21 (1) preempt or otherwise affect the application
22 of the Arms Export Control Act (22 U.S.C. 2751 et
23 seq.), the Export Administration Act of 1979 (50
24 U.S.C. App. 2401 et seq.), or the International

1 Emergency Economic Powers Act (50 U.S.C. 1701
2 et seq.) or any regulations promulgated thereunder;

3 (2) affect foreign intelligence activities of the
4 United States; or

5 (3) negate or diminish any intellectual property
6 protections under the laws of the United States or
7 of any State.

8 **SEC. 603. FBI TECHNICAL SUPPORT.**

9 There are authorized to be appropriated for the Tech-
10 nical Support Center in the Federal Bureau of Investiga-
11 tion, established pursuant to section 811(a)(1) of the
12 Antiterrorism and Effective Death Penalty Act of 1996
13 (Public Law 104–132)—

14 (1) \$25,000,000 for fiscal year 2000 for build-
15 ing and personnel costs;

16 (2) \$20,000,000 for fiscal year 2001 for per-
17 sonnel and equipment costs;

18 (3) \$15,000,000 for fiscal year 2002; and

19 (4) \$15,000,000 for fiscal year 2003.

20 **SEC. 604. SEVERABILITY.**

21 If any provision of this Act or the amendments made
22 by this Act, or the application thereof, to any person or
23 circumstances is held invalid by a court of the United
24 States, the remainder of this Act or such amendments,

1 and the application thereof, to other persons or cir-
2 cumstances shall not be affected thereby.

○