

Calendar No. 263

106TH CONGRESS
1ST Session

S. 798

[Report No. 106-142]

A BILL

To promote electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protection of national security, and for other purposes.

August 5, 1999

Reported without amendment

Calendar No. 263106TH CONGRESS
1ST SESSION**S. 798****[Report No. 106-142]**

To promote electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protection of national security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 14, 1999

Mr. MCCAIN (for himself, Mr. BURNS, Mr. WYDEN, Mr. LEAHY, Mr. ABRAHAM, Mr. KERRY, Mrs. HUTCHISON, and Mr. FEINGOLD) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

AUGUST 5, 1999

Reported by Mr. MCCAIN, without amendment

A BILL

To promote electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protection of national security, 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Promote Reliable On-
3 Line Transactions to Encourage Commerce and Trade
4 (PROTECT) Act of 1999”.

5 **SEC. 2. PURPOSES.**

6 The purposes of this Act are—

7 (1) to promote electronic growth foster elec-
8 tronic commerce;

9 (2) create consumer confidence in electronic
10 commerce;

11 (3) meet the needs of businesses and individuals
12 using electronic networks;

13 (4) prevent crime; and

14 (5) improve national security

15 by facilitating the widespread use of encryption and
16 assisting the United States Government in devel-
17 oping the capability to respond to the challenges
18 posed by new technological developments.

19 **SEC. 3. FINDINGS.**

20 Congress finds the following:

21 (1) The ability to digitize information makes
22 carrying out tremendous amounts of commerce and
23 personal communication electronically possible.

24 (2) Miniaturization, distributed computing, and
25 reduced transmission costs make communication via
26 electronic networks a reality.

1 (3) The explosive growth in the Internet and
2 other computer networks reflects the potential
3 growth of electronic commerce and personal commu-
4 nication.

5 (4) The Internet and the global information in-
6 frastructure have the potential to revolutionize the
7 way individuals and businesses conduct business.

8 (5) The full potential of the Internet for the
9 conduct of business cannot be realized as long as it
10 is an insecure medium in which confidential business
11 information and sensitive personal information re-
12 main at risk of unauthorized viewing, alteration, and
13 use.

14 (6) The United States' critical infrastructures
15 increasingly rely on vulnerable commercial informa-
16 tion systems and electronic networks and represent
17 a growing risk to national security and public safety
18 because the security and privacy of those systems
19 and networks is not assured.

20 (7) Encryption of information enables busi-
21 nesses and individuals to protect themselves, their
22 commercial information and networks, and the
23 United States' critical infrastructures against unau-
24 thorized viewing, alteration, and abuse ensuring the

1 security, confidentiality, authenticity, and integrity
2 of information.

3 (8) American computer software and hardware,
4 communications, and electronics businesses are lead-
5 ing the world technology revolution, and the Amer-
6 ican information technology industry is a vital sector
7 of the United States economy. These businesses have
8 developed in the commercial marketplace, and are
9 prepared to offer immediately to computer users
10 worldwide, a variety of communications and com-
11 puter hardware and software that provide strong, ro-
12 bust, and easy-to-use encryption.

13 (9) Notwithstanding American preeminence in
14 information technology, many foreign companies cur-
15 rently manufacture products and services that are
16 comparable in quality and capabilities to United
17 States products and frequently provide stronger
18 encryption. These foreign companies are competing
19 fiercely with United States companies for sales not
20 only of the encryption product or service, but also
21 for the ultimate product that uses the encryption ca-
22 pability, including applications ranging from online
23 banking to electronic mail to banking.

24 (10) The leading survey of available encryption
25 products reports that, as of December, 1997, there

1 were 656 foreign encryption products (out of 1619
2 encryption products produced worldwide) available
3 from 474 vendors in 29 different foreign countries.

4 (11) To promote economic growth, foster elec-
5 tronic commerce, meet the needs of businesses and
6 individuals using electronic networks, prevent crime,
7 and improve national security, Americans should be
8 free to continue using lawfully any encryption prod-
9 ucts and programs, and American companies should
10 be free to sell, license, or otherwise distribute such
11 encryption products and programs worldwide so long
12 as national security is not put at risk.

13 (12) The United States government should pro-
14 mote the use of the United States encryption prod-
15 ucts and expedite its work with the industry to up-
16 date the United States Data Encryption Standard
17 (DES).

18 (13) NIST has proposed requirements and es-
19 tablished procedures for adopting a new, stronger,
20 private sector—developed Advanced Encryption
21 Standard (AES).

22 (14) Similar to DES, it is anticipated that AES
23 will become an international encryption standard
24 adopted by individuals and companies worldwide.

1 (15) NIST has requested candidate algorithms,
2 evaluated candidate algorithms, and encouraged
3 public comment at each step of the process. NIST's
4 open and public process for developing and testing
5 the new AES should be applauded and supported.

6 (16) Further demonstrating the worldwide
7 availability, use, and sophistication of encryption
8 abroad, only 5 of the 15 AES candidate algorithms
9 submitted to NIST for evaluation that complied with
10 all requirements and procedures for submission were
11 proposed by companies and individuals in the United
12 States. The remaining 10 candidate algorithms were
13 proposed by individuals and companies from 11 dif-
14 ferent countries (Australia's LOKI97; Belgium's
15 RIJNDAEL; Canada's CAST-256 and DEAL;
16 Costa Rica's FROG; France's DFC; Germany's MA-
17 GENTA; Japan's E2; Korea's CRYPTON; and the
18 United Kingdom, Israel, and Norway's SERPENT
19 algorithms).

20 (17) NIST's efforts to create the AES to re-
21 place DES are important to the development of ade-
22 quate global information security to a degree that
23 Congress should explicitly authorize and support
24 NIST's efforts and establish a deadline of January
25 1, 2002, for finalizing the new standard.

1 (18) Once NIST finalizes AES, the Federal
2 Government should permit all United States prod-
3 ucts meeting the new AES standards or its equiva-
4 lent to be exported worldwide to ensure global secu-
5 rity and to permit United States companies to com-
6 pete effectively with their foreign competitors con-
7 sistent with the national security requirements of the
8 United States.

9 (19) The United States Government has legiti-
10 mate law enforcement and national security objec-
11 tives, which can be met by permitting American
12 companies to compete globally, while at the same
13 time recognizing the challenges to law enforcement
14 and national security posed by quickly advancing
15 technological developments and providing for re-
16 search, development, and adoption of new technology
17 to respond to these challenges.

18 (20) As part of its efforts to fight crime with
19 technology and ensure the safety of commercial net-
20 works, the United States government should estab-
21 lish a mechanism for facilitating communications
22 with experts in information security industries, in-
23 cluding cryptographers, engineers, software pub-
24 lishers, and others involved in the design and devel-
25 opment of information security products and should

1 ensure that such sums as necessary are appropriated
2 to ensure and enhance national security and law en-
3 forcement.

4 (21) The United Government also should ex-
5 pand and expedite its computer security research ac-
6 tivities at NIST and the Federal laboratories, work
7 with industry to recommend priority activities at
8 university research facilities, and fund scholarships
9 in information security.

10 **SEC. 4. DEFINITIONS.**

11 In this Act:

12 (1) **COMPUTER HARDWARE.**—The term “com-
13 puter hardware” includes computer systems, equip-
14 ment, application-specific assemblies, smart cards,
15 modules, integrated circuits, printed circuit board
16 assemblies, and devices that incorporate 1 or more
17 microprocessor-based central processing units that
18 are capable of accepting, storing, processing, or pro-
19 viding output of data.

20 (2) **ENCRYPT AND ENCRYPTION.**—The term
21 “encrypt” and “encryption” means the scrambling
22 (and descrambling) of wire communications, elec-
23 tronic communications, or electronically stored infor-
24 mation, using mathematical formulas or algorithms
25 to preserve the confidentiality, integrity, or authen-

1 ticity of, and prevent unauthorized recipients from
2 accessing or altering, such communications or infor-
3 mation.

4 (3) ENCRYPTION PRODUCT.—The term
5 “encryption product”—

6 (A) means computer hardware, computer
7 software, or technology with encryption capa-
8 bilities; and

9 (B) includes any subsequent version of or
10 update to an encryption product, if the
11 encryption capabilities are not changed.

12 (4) EXPORTABLE.—The term “exportable”
13 means the ability to transfer, ship, or transmit to
14 foreign users.

15 (5) GENERALLY AVAILABLE OR GENERAL
16 AVAILABILITY.—The terms “generally available” or
17 “general availability” mean—

18 (A) in the case of computer hardware or
19 computer software (including encryption prod-
20 ucts), computer hardware, or computer software
21 that is—

22 (i) distributed via the Internet;

23 (ii) widely offered for sale, license, or
24 transfer (without regard to whether it is
25 offered for consideration), including over-

1 the-counter retail sales, mail order trans-
2 actions, telephone order transactions, elec-
3 tronic distribution, or sale on approval;

4 (iii) preloaded on computer hardware
5 that is widely available; or

6 (iv) assembled from computer hard-
7 ware or computer software components
8 that are generally available;

9 (B) not designed, developed, or tailored by
10 the manufacturer for specific purchasers, except
11 that the purchaser or user may—

12 (i) supply certain installation param-
13 eters needed by the computer hardware or
14 computer software to function properly
15 with the computer system of the user or
16 purchaser; or

17 (ii) select from among options con-
18 tained in the computer hardware or com-
19 puter software; and

20 (C) are available in more than 1 country
21 through a means described in subparagraph
22 (A).

23 (6) KEY.—The term “key” means the variable
24 information used in a mathematical formula, code,
25 or algorithm, or any component thereof, used to

1 decrypt wire communications, electronic communica-
2 tions, or electronically stored information, that has
3 been encrypted.

4 (7) LICENSE EXCEPTION.—The term “license
5 exception” means an authorization by the Bureau of
6 Export Administration of the Department of Com-
7 merce that allows the export or re-export, under
8 stated conditions, of items subject to the Export Ad-
9 ministration Regulations that otherwise would re-
10 quire a license.

11 (8) NIST.—The term “NIST” means the Na-
12 tional Institute of Standards and Technology in the
13 Department of Commerce.

14 (9) ON-LINE MERCHANT.—The term “on-line
15 merchant” means either a person or a company or
16 other entity engaged in commerce that, as part of its
17 business, uses electronic means to conduct commer-
18 cial transactions in goods (including, but not limited
19 to, software and all other forms of digital content)
20 or services, whether delivered in tangible or elec-
21 tronic form.

22 (10) PERSON.—The term “person” has the
23 meaning given the term in section 2510(1) of title
24 1, United States Code.

1 (11) PUBLICLY AVAILABLE OR PUBLIC AVAIL-
2 ABILITY.—The terms “publicly available” or “public
3 availability” mean—

4 (A) information that is generally accessible
5 to the interested public in any form; or

6 (B) technology and software that are al-
7 ready published or will be published, arise dur-
8 ing, or result from fundamental research, are
9 educational, or are included in certain patent
10 applications.

11 (12) RECOVERABLE PRODUCT.—The term “re-
12 coverable product” means an encryption product
13 that—

14 (A) incorporates an operator-controlled
15 management interface enabling real-time access
16 to specified network traffic prior to encryption,
17 or after decryption, at a designated access point
18 under the control of the network owner or oper-
19 ator (utilizing a protocol such as IPsec);

20 (B) permits access to data prior to
21 encryption, or after decryption, at a server
22 under the control of a network owner or oper-
23 ator (utilizing a protocol such as SSL, TLS, or
24 Kerberos);

1 (C) includes a key or data recovery system
2 which, when activated, enables a system admin-
3 istrator or user to recover plaintext or keys to
4 decrypt data transmitted or stored in encrypted
5 form; or

6 (D) offers the system administrator or
7 end-user the capability to create a duplicate key
8 (or keys) for archival and other purposes.

9 (13) SECRETARY.—The term “Secretary”
10 means the Secretary of Commerce.

11 (14) STATE.—The term “State” means any
12 State of the United States and includes the District
13 of Columbia and any commonwealth, territory, or
14 possessions of the United States.

15 (15) STRATEGIC PARTNERS.—The term “stra-
16 tegic partners” means 2 or more entities that—

17 (A) have a business need to share the pro-
18 prietary information of 1 or more United States
19 companies; and

20 (B) are contractually bound to one an-
21 other; or

22 (C) have an established pattern on con-
23 tinuing or recurring contractual relations.

24 (16) TECHNICAL ASSISTANCE.—The term
25 “technical assistance” includes assistance such as in-

1 instructions, skills training, working knowledge, and
2 consulting services, and may involve transfer of tech-
3 nical data.

4 (17) TECHNICAL DATA.—The term “technical
5 data” may include data such as blueprints, plans,
6 diagrams, models, formulae, tables, engineering de-
7 signs and specifications, manuals, and instructions
8 written or recorded on other media or devices such
9 as disk, tape, or read-only memories.

10 (18) TECHNICAL REVIEW.—The term “tech-
11 nical review” means a review by the Secretary of an
12 encryption product, based on information about a
13 product’s encryption capabilities supplied by the
14 manufacturer, that an encryption product works as
15 represented.

16 (19) UNITED STATES PERSON.—The term
17 “United States person” means any—

18 (A) United States citizen; or

19 (B) legal entity that—

20 (i) is organized under the laws of the
21 United States, or any State, the District
22 of Columbia, or any commonwealth, terri-
23 tory, or possession of the United States;
24 and

1 (ii) has its principal place of business
2 in the United States.

3 (20) UNITED STATES SUBSIDIARY.—The term
4 “United States subsidiary” means—

5 (A) a foreign branch of a United States
6 company; or

7 (B) a foreign subsidiary or entity of a
8 United States entity in which—

9 (i) a United States company or entity
10 beneficially owns or controls (whether di-
11 rectly or indirectly) 25 percent or more of
12 the voting securities of the foreign sub-
13 sidiary or entity, if no other person owns
14 or controls (whether directly or indirectly)
15 an equal or larger percentage;

16 (ii) the foreign subsidiary or entity is
17 operated by a United States company or
18 entity pursuant to the provisions of an ex-
19 clusive management contract;

20 (iii) the majority of the members of
21 the Board of Directors of the foreign sub-
22 sidiary or entity also are members of the
23 comparable governing body of the United
24 States company or entity;

1 (iv) a United States company or enti-
 2 ty has the authority to appoint the major-
 3 ity of the members of the Board of Direc-
 4 tors of the foreign subsidiary; or

5 (v) a United States company or entity
 6 has the authority to appoint the Chief Op-
 7 erating officer of the foreign subsidiary or
 8 entity.

9 **TITLE I—DOMESTIC**
 10 **ENCRYPTION PROVISIONS**

11 **SEC. 101. DEVELOPMENT AND DEPLOYMENT OF**
 12 **ENCRYPTION A VOLUNTARY PRIVATE SEC-**
 13 **TOR ACTIVITY.**

14 (a) STATEMENT OF POLICY.—The use, development,
 15 manufacture, sale, distribution, and importation of
 16 encryption products, standards, and services for purposes
 17 of assuring the confidentiality, authenticity, or integrity
 18 of electronic information shall be voluntary and market
 19 driven.

20 (b) LIMITATION ON REGULATION.—Neither the Fed-
 21 eral Government nor a State may establish any conditions,
 22 ties, or links between encryption products, standards, and
 23 services used for confidentiality, and those used for au-
 24 thenticity or integrity purposes.

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

2 Except as otherwise provided by this Act, it is lawful
3 for any person within any State, and for any United
4 States person in a foreign country, to develop, manufac-
5 ture, sell, distribute, import, or use any encryption prod-
6 uct, regardless of the encryption algorithm selected,
7 encryption length chosen, existence of key recovery, or
8 other plaintext access capability, or implementation or me-
9 dium used.

10 **SEC. 103. MANDATORY GOVERNMENT ACCESS TO**
11 **PLAINTEXT PROHIBITED.**

12 (a) IN GENERAL.—No department, agency, or instru-
13 mentality of the United States or of any State may—

- 14 (1) require that;
15 (2) set standards for;
16 (3) condition any approval on;
17 (4) create incentives for; or
18 (5) tie any benefit to,

19 a requirement that, a decryption key, access to a
20 key, key recovery information, or any other plaintext
21 access capability be—

22 (A) required to be built into computers
23 hardware or software for any purpose;

24 (B) given to any other person (including a
25 department, agency, or instrumentality of the
26 United States or an entity in the private sector

1 that may be certified or approved by the United
2 States or a State); or

3 (C) retained by the owner or user of an
4 encryption key or any other person, other than
5 for encryption products for the use of the
6 United States Government or a State govern-
7 ment.

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

15 **TITLE II—GOVERNMENT** 16 **PROCUREMENT**

17 **SEC. 201. POLICY.**

18 It is the policy of the United States—

19 (1) to permit the public to interact with govern-
20 ment through commercial networks and infrastruc-
21 ture; and

22 (2) to protect the privacy and security of any
23 electronic communication from, or stored informa-
24 tion obtained from, the public.

1 **SEC. 202. FEDERAL PURCHASES OF ENCRYPTION PROD-**
2 **UCTS.**

3 (a) **IN GENERAL.**—Any department, agency, or in-
4 strumentality of the United States may purchase
5 encryption products for use by officers and employees of
6 the United States to the extent and in the manner author-
7 ized by law.

8 (b) **INTEROPERABILITY REQUIRED.**—No department,
9 agency, or instrumentality of the United States, nor any
10 department, agency, or political subdivision of a State,
11 may purchase an encryption product for its use unless the
12 product will interoperate with other commercially-available
13 encryption products, including products without a
14 decryption key, access to a key, key recovery information,
15 or any other plaintext access capability.

16 (c) **CITIZENS NOT REQUIRED TO PURCHASE SPECI-**
17 **IFIED PRODUCT.**—No department, agency, or instrumen-
18 tality of the United States, nor any department, agency,
19 or political subdivision of a State, may require any person
20 in the private sector to use any particular encryption prod-
21 uct or methodology, including products with a decryption
22 key, access to a key, key recovery information, or any
23 other plaintext access capability, to communicate with, or
24 transact business with, the government.

1 **TITLE III—ADVANCED**
2 **ENCRYPTION STANDARD**

3 **SEC. 301. DEADLINE FOR FINAL SELECTION OF ALGO-**
4 **RITHM OR ALGORITHMS BY NIST.**

5 (a) **AES PROCESS.**—The NIST shall continue and
6 complete the AES process initiated on January 2, 1997,
7 including—

- 8 (1) establishing performance requirements,
9 (2) setting procedures for submitting, testing,
10 evaluating, and judging proposals; and
11 (3) finally selecting one or more new private
12 sector-developed encryption algorithms.

13 (b) **DEADLINE.**—Notwithstanding subsection (a),
14 NIST shall make a final selection of one or more new pri-
15 vate sector-developed encryption algorithms by January 1,
16 2002.

17 **SEC. 302. COMMERCE DEPARTMENT ENCRYPTION STAND-**
18 **ARDS AND EXPORTS AUTHORITY RE-**
19 **STRICTED.**

20 (a) **REGULATORY AUTHORITY.**—Except as otherwise
21 provided in this Act, the Secretary of Commerce may not
22 promulgate or enforce any regulation, adopt any standard,
23 or carry out any policy that establishes an encryption
24 standard for use by businesses or other entities other than

1 for computer systems operated by a department, agency,
2 or other entity of the United States government.

3 (b) EXPORT AUTHORITY.—Except as otherwise pro-
4 vided in this Act, the Secretary of Commerce may not pro-
5 mulgate or enforce any regulation, adopt any standard,
6 or carry out any policy relating to encryption that has the
7 effect of imposing government-designed encryption stand-
8 ards on the private sector by restricting the export of
9 encryption products.

10 **TITLE IV—IMPROVEMENT OF**
11 **GOVERNMENTAL TECHNO-**
12 **LOGICAL CAPABILITY**

13 **SEC. 401. INFORMATION TECHNOLOGY LABORATORY.**

14 Section 20(b) of the National Institute of Standards
15 and Technology Act (15 U.S.C. 278g–3(b)) is amended—

16 (1) by striking “and” at the end of paragraph
17 (4);

18 (2) by striking “policy.” in paragraph (5) and
19 inserting “policy;” and

20 (3) by adding at the end thereof the following:

21 “(6) to obtain information regarding the most
22 current information security hardware, software,
23 telecommunications, and other electronic capabilities;

1 “(7) to research and develop new and emerging
2 techniques and technologies to facilitate lawful ac-
3 cess to communications and electronic information;

4 “(8) to research and develop methods to detect
5 and prevent unwanted intrusions into commercial
6 computer networks, particularly those interconnected
7 with computer systems of the United States govern-
8 ment;

9 “(9) to provide assistance in responding to in-
10 formation security threats and vulnerabilities at the
11 request of other departments, agencies, and instru-
12 mentalities of the United States and State govern-
13 ments; and

14 “(10) to facilitate the development and adop-
15 tion of the best information security practices by de-
16 partments, agencies, and instrumentalities of the
17 United States, the States, and the private sector.”.

18 **SEC. 402. ADVISORY BOARD ON COMPUTER SYSTEM SECU-**
19 **RITY AND PRIVACY.**

20 Section 21(b) of the National Institute of Standards
21 and Technology Act (15 U.S.C. 278g-4(b)) is amended—

22 (1) by redesignating paragraphs (2) and (3) as
23 paragraphs (4) and (5), respectively; and

24 (2) by inserting after paragraph (1) the fol-
25 lowing:

1 “(2) to provide a forum for communication and
2 coordination between industry and the Federal Gov-
3 ernment regarding information security issues;

4 “(3) to foster the aggregation and dissemina-
5 tion of general, nonproprietary, and non-confidential
6 developments in important information security tech-
7 nologies, including encryption, by regularly reporting
8 that information to appropriate Federal agencies to
9 keep law enforcement and national security agencies
10 abreast of emerging technologies so they are able ef-
11 fectively to meet their responsibilities;”.

12 **SEC. 403. AUTHORIZATION OF APPROPRIATIONS.**

13 There are authorized to be appropriated to such de-
14 partments and agencies as may be appropriate such sums
15 as may be necessary to ensure that United States law en-
16 forcement agencies and agencies responsible for national
17 security are able to complete any missions or goals author-
18 ized in law regardless of technological advancements in
19 encryption and digital technology.

20 **TITLE V—EXPORT OF**
21 **ENCRYPTION PRODUCTS.**

22 **SEC. 501. COMMERCIAL ENCRYPTION PRODUCTS.**

23 (a) IN GENERAL.—This title applies to all encryption
24 products, without regard to the encryption algorithm se-
25 lected, encryption key chosen, exclusion of plaintext access

1 capability, or implementation or medium used, except
2 those encryption products specifically designed or modified
3 for military use (including command, control, and intel-
4 ligence applications).

5 (b) **AUTHORITY OF SECRETARY OF COMMERCE.**—
6 Subject to the other provisions of this title, and notwith-
7 standing any other provision of law, the Secretary of Com-
8 merce has exclusive authority to control the exportation
9 of encryption products described in subsection (a). In exer-
10 cising that authority, the Secretary shall consult with the
11 Secretary of State and the Secretary of Defense.

12 **SEC. 502. PRESIDENTIAL AUTHORITY.**

13 (a) **TERRORIST AND EMBARGO CONTROLS.**—Nothing
14 in this Act limits the authority of the President under—

15 (1) the Trading with the Enemy Act (50 U.S.C.
16 App. 1 et seq.); or

17 (2) the International Emergency Economic
18 Powers Act (50 U.S.C. 1701 et seq.), but only to the
19 extent that the authority of that Act is not exercised
20 to extend controls imposed under the Export Admin-
21 istration Act of 1979 (50 U.S.C. 2401 et seq.)—

22 (A) to prohibit the export of encryption
23 products to any country, corporation, or other
24 entity that has been determined to—

1 (i) provide support for acts of ter-
2 rorism; or

3 (ii) pose an immediate threat to na-
4 tional security; or

5 (B) to impose an embargo on exports to,
6 or imports from, a specific country, corporation,
7 or entity.

8 (b) SPECIAL DENIALS FOR SPECIFIC REASONS.—

9 The Secretary of Commerce shall prohibit the exportation
10 of particular encryption products to an individual or orga-
11 nization in a foreign country identified by the Secretary
12 if the Secretary determines that there is substantial evi-
13 dence that the encryption products may be used or modi-
14 fied for military or terrorist use, including acts against
15 the national security of, public safety of, or the integrity
16 of the transportation, communications, or other essential
17 systems of interstate commerce in, the United States.

18 (c) OTHER EXPORT CONTROLS.—An encryption
19 product is subject to any export control imposed on that
20 product for any reason other than the existence of
21 encryption capability. Nothing in this title alters the Sec-
22 retary of Commerce's ability to control exports of products
23 for reasons other than encryption.

1 **SEC. 503. EXPORTATION OF ENCRYPTION PRODUCTS WITH**
2 **NOT MORE THAN 64—BIT KEY LENGTH.**

3 An encryption product that utilizes a key length or
4 64 bits or less, may be exported without an export license
5 or an export license exception, and without any other re-
6 striction (other than a restriction imposed under this
7 title).

8 **SEC. 504. EXPORTABILITY OF CERTAIN ENCRYPTION PROD-**
9 **UCTS UNDER A LICENSE EXCEPTION.**

10 (a) **LICENSE EXCEPTIONS.**—Except as otherwise
11 provided under this title, the export or re-export of the
12 following products shall be exportable under license excep-
13 tion:

14 (1) Recoverable products.

15 (2) Encryption products to legitimate and re-
16 sponsible entities or organizations and their strategic
17 partners, including—

18 (A) firms whose shares are publicly traded
19 in global markets;

20 (B) firms subject to a governmental regu-
21 latory scheme;

22 (C) United States subsidiaries or affiliates
23 of United States corporations;

24 (D) firms or organizations that are re-
25 quired by law to maintain plaintext records of
26 communications or otherwise maintain such

1 records as part of their normal business prac-
2 tice;

3 (E) firms or organizations that are audited
4 annually under widely accepted accounting prin-
5 ciples;

6 (F) strategic partners of United States
7 companies; and

8 (G) on-line merchants who use encryption
9 products to support electronic commerce, in-
10 cluding protecting commercial transactions as
11 well as non-public information exchange nec-
12 essary to support such transactions.

13 (3) Encryption products sold or licensed to for-
14 eign governments that are members of the North At-
15 lantic Treaty Organization, Organization for Eco-
16 nomic Cooperation and Development, and Associa-
17 tion of Southeast Asian Nations.

18 (4) Any computer hardware or computer soft-
19 ware that does not itself provide encryption capabili-
20 ties, but that incorporates or employs in any form
21 interface mechanisms for interaction with other com-
22 puter hardware and computer software, including
23 encryption products.

24 (5) Any technical assistance or technical data
25 associated with the installation and maintenance of

1 encryption products, or products incorporating, ena-
2 bling, or employing encryption products, if such
3 products are exportable under this title.

4 (b) LICENSE EXCEPTION PROCESSING PERIOD IN-
5 CLUDING ONE-TIME TECHNICAL REVIEW.—Encryption
6 products and related computer services shall be eligi-
7 ble for a license exception after a one-time technical re-
8 view. Exporters' requests for license exceptions, including
9 the one-time technical review, must be processed within
10 15 working days from receipt of a request. If the exporter
11 is not contacted within this 15-day processing period, the
12 exporter's request for a license exception will be deemed
13 granted, and the exporter may export the encryption prod-
14 ucts or related computer services under the license excep-
15 tion.

16 **SEC. 505. EXPORTABILITY OF ENCRYPTION PRODUCTS EM-**
17 **PLOYING A KEY LENGTH GREATER THAN 64-**
18 **BITS.**

19 (a) EXPORT RELIEF FOR ENCRYPTION PRODUCTS.—
20 Encryption products, or products that incorporate or em-
21 ploy in any form, implementation, or medium an
22 encryption product, are exportable under a license excep-
23 tion if—

1 (1) the Secretary determines that the product
2 or service is exportable under the Export Adminis-
3 tration Act of 1979 (50 U.S.C. 2401 et seq.); or

4 (2) the Encryption Export Advisory Board de-
5 scribed in subsection (b) determines, and the Sec-
6 retary agrees, that the product or service is—

7 (A) generally available;

8 (B) publicly available; or

9 (C) an encryption product utilizing the
10 same or greater key length or otherwise pro-
11 viding comparable security is, or will be within
12 the next 12 months generally or widely avail-
13 able outside the United States from a foreign
14 supplier.

15 (b) BOARD DETERMINATION OF EXPORTABILITY.—

16 (1) ENCRYPTION EXPORT ADVISORY BOARD.—

17 There is hereby established an Encryption Export
18 Advisory Board comprised of—

19 (A) a Chairman, who shall be the Under
20 Secretary of Commerce for Export Administra-
21 tion;

22 (B) 7 individuals appointed by the Presi-
23 dent, as follows—

24 (i) 1 representative from the National
25 Security Agency;

1 (ii) 1 representative from the Central
2 Intelligence Agency;

3 (iii) 1 representative from the Office
4 of the President; and

5 (iv) 4 representatives from the private
6 sector who have expertise in the develop-
7 ment, operation, or marketing of informa-
8 tion technology products; and

9 (C) 4 representatives from the private sec-
10 tor who have expertise in the development, op-
11 eration, or marketing of information technology
12 products appointed by the Congress, as
13 follows—

14 (i) 1 representative appointed by the
15 Majority Leader of the Senate;

16 (ii) 1 representative appointed by the
17 Minority Leader of the Senate;

18 (iii) 1 representative appointed by the
19 Speaker of the House of Representatives;
20 and

21 (iv) 1 representative appointed by the
22 Minority Leader of the House of Rep-
23 resentatives.

24 (2) PURPOSE.—The Board shall evaluate and
25 make recommendations by majority vote within 30

1 days with respect to general availability, public avail-
2 ability, or foreign availability whenever an applica-
3 tion for a license exception based on general avail-
4 ability, public availability, or foreign availability has
5 been submitted to the Secretary.

6 (3) MEETINGS.—The Board shall meet at the
7 call of the Under Secretary upon a request for a de-
8 termination, but at least every 30 days if a request
9 is pending. The Federal Advisory Committee Act (5
10 U.S.C. App.) does not apply to the Board or to
11 meetings held by the Board under this subsection.

12 (4) ACTION BY THE SECRETARY.—The Board
13 shall make recommendations to the Secretary. The
14 Secretary shall specifically approve or disapprove of
15 each finding of availability within 30 days of receiv-
16 ing the recommendation and shall notify the Board
17 and publish the finding in the Federal Register. The
18 Secretary shall explain in detail the reasons for any
19 disapproval, including why and how continued con-
20 trols will be effective in achieving their purpose and
21 the amount of lost sales and loss in market share of
22 United States encryption products.

23 (5) JUDICIAL REVIEW.—Notwithstanding any
24 other provision of law, a decision by the Secretary
25 disapproving of a Board finding of availability shall

1 be subject to judicial review under the Administra-
2 tive Procedure Act (5 U.S.C. 551 et seq.).

3 (6) PRESIDENTIAL OVERRIDE.—The Board
4 shall report to the President within 30 days after
5 each meeting. The President may override any
6 Board determination of exportability and control the
7 export and re-export of specified encryption products
8 to specific countries or individuals if he determines
9 that such exports or re-exports would harm United
10 States national security, including United States ca-
11 pabilities in fighting drug trafficking, terrorism, or
12 espionage. If the President overrides a Board deter-
13 mination of exportability and decides to control the
14 export or re-export of any encryption product, the
15 President must inform the Board and Congress and
16 detail the reasons for such controls within 30 days
17 of the determination. The action of the president
18 under this paragraph is not subject to judicial re-
19 view.

20 (c) RELY ON DETERMINATION OF BOARD.—The
21 manufacturer or exporter of an encryption product or a
22 product incorporating or employing an encryption product
23 may rely upon the Board's determination that the product
24 is generally available or publicly available or if a com-
25 parable foreign encryption product is available, and shall

1 not be held liable or responsible or subject to sanctions
2 for any export of such products under the license excep-
3 tion.

4 (d) LICENSE EXCEPTION PROCESSING PERIOD IN-
5 CLUDING ONE-TIME TECHNICAL REVIEW.—Encryption
6 products and related computer services shall be made eligi-
7 ble for a license exception after a one-time technical re-
8 view. Exporters' requests for license exceptions, including
9 the one-time technical review, must be processed within
10 15 working days from receipt of a request. If the exporter
11 is not contacted within this 15—day processing period, the
12 exporter's request for a license exception will be deemed
13 granted, and the exporter may export the encryption prod-
14 ucts or related computer services under the license excep-
15 tion.

16 (e) GRANDFATHERING OF PRIOR DETERMINA-
17 TIONS.—Any determination by the Secretary prior to en-
18 actment of this Act that an encryption product with great-
19 er than a 64-bit key length, or product incorporating or
20 employing such an encryption product, and related serv-
21 ices, is eligible for export and re-export either without a
22 license or under a license, a license exception, or an
23 encryption licensing arrangement will remain in effect
24 after passage of this Act.

1 **SEC. 506. EXPORTABILITY OF ENCRYPTION PRODUCTS EM-**
2 **PLOYING AES OR ITS EQUIVALENT.**

3 Upon adoption of the AES, but not later than Janu-
4 ary 1, 2002, the Secretary may no longer impose United
5 States encryption export controls on encryption products
6 if the encryption algorithm and key length employed were
7 incorporated in the AES, or have an equivalent strength,
8 and such product shall be exportable without the need for
9 an export license or license exception, and without restric-
10 tions other than those permitted under this Act.

11 **SEC. 507. ELIMINATION OF REPORTING REQUIREMENTS.**

12 The Secretary may not impose any reporting require-
13 ments on any encryption product not subject to United
14 States export controls or exported under a license excep-
15 tion.