106TH CONGRESS
1ST SESSION

S. 798

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, and Mr. KERRY) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

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

SEC. 2. PURPOSES.

The purposes of this Act are—

(1) to promote electronic growth foster electronic commerce;

(2) create consumer confidence in electronic commerce;

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

(4) prevent crime; and

(5) improve national security

by facilitating the widespread use of encryption and assisting the United States Government in developing the capability to respond to the challenges posed by new technological developments.

SEC. 3. FINDINGS.

Congress finds the following:

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

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

(3) The explosive growth in the Internet and other computer networks reflects the potential growth of electronic commerce and personal communication.

(4) The Internet and the global information infrastructure have the potential to revolutionize the way individuals and businesses conduct business.

(5) The full potential of the Internet for the conduct of business cannot be realized as long as it is an insecure medium in which confidential business information and sensitive personal information remain at risk of unauthorized viewing, alteration, and use.

(6) The United States critical infrastructures increasingly rely on vulnerable commercial information systems and electronic networks and represent a growing risk to national security and public safety because the security and privacy of those systems and networks is not assured.

(7) Encryption of information enables businesses and individuals to protect themselves, their commercial information and networks, and the United States critical infrastructures against unauthorized viewing, alteration, and abuse ensuring the security, confidentiality, authenticity, and integrity of information.

(8) American computer software and hardware, communications, and electronics businesses are leading the world technology revolution, and the Amer-

ican information technology industry is a vital sector of the United States economy. These businesses have developed in the commercial marketplace, and are prepared to offer immediately to computer users worldwide, a variety of communications and computer hardware and software that provide strong, robust, and easy-to-use encryption.

(9) Notwithstanding American preeminence in information technology, many foreign companies currently manufacture products and services that are comparable in quality and capabilities to United States products and frequently provide stronger encryption. These foreign companies are competing fiercely with United States companies for sales not only of the encryption product or service, but also for the ultimate product that uses the encryption capability, including applications ranging from online banking to electronic mail to banking.

(10) The leading survey of available encryption products reports that, as of December, 1997, there were 656 foreign encryption products (out of 1619 encryption products produced worldwide) available from 474 vendors in 29 different foreign countries.

(11) To promote economic growth, foster electronic commerce, meet the needs of businesses and

individuals using electronic networks, prevent crime, and improve national security, Americans should be free to continue using lawfully any encryption products and programs, and American companies should be free to sell, license, or otherwise distribute such encryption products and programs worldwide so long as national security is not put at risk.

(12) The United States government should promote the use of the United States encryption products and expedite its work with the industry to update the United States Data Encryption Standard (DES).

(13) NIST has proposed requirements and established procedures for adopting a new, stronger, private sector—developed Advanced Encryption Standard (AES).

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

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

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

(17) NIST's efforts to create the AES to replace DES are important to the development of adequate global information security to a degree that Congress should explicitly authorize and support NIST's efforts and establish a deadline of January 1, 2002, for finalizing the new standard.

(18) Once NIST finalizes AES, the Federal Government should permit all United States products meeting the new AES standards or its equivalent to be exported worldwide to ensure global security and to permit United States companies to com-

pete effectively with their foreign competitors consistent with the national security requirements of the United States.

(19) The United States Government has legitimate law enforcement and national security objectives, which can be met by permitting American companies to compete globally, while at the same time recognizing the challenges to law enforcement and national security posed by quickly advancing technological developments and providing for research, development, and adoption of new technology to respond to these challenges.

(20) As part of its efforts to fight crime with technology and ensure the safety of commercial networks, the United States Government should establish a mechanism for facilitating communications with experts in information security industries, including cryptographers, engineers, software publishers, and others involved in the design and development of information security products and should ensure that such sums as necessary are appropriated to ensure and enhance national security and law enforcement.

(21) The United States Government also should expand and expedite its computer security research

activities at NIST and the Federal laboratories, work with industry to recommend priority activities at university research facilities, and fund scholarships in information security.

SEC. 4. DEFINITIONS.

In this Act:

(1) COMPUTER HARDWARE.—The term ''computer hardware'' includes computer systems, equipment, application-specific assemblies, smart cards, modules, integrated circuits, printed circuit board assemblies, and devices that incorporate 1 or more microprocessor-based central processing units that are capable of accepting, storing, processing, or providing output of data.

(2) ENCRYPT AND ENCRYPTION.—The term ''encrypt'' and ''encryption'' means the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information.

(3) ENCRYPTION PRODUCT.—The term ''encryption product''—

(A) means computer hardware, computer software, or technology with encryption capabilities; and

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

(4) EXPORTABLE.—The term ''exportable'' means the ability to transfer, ship, or transmit to foreign users.

(5) GENERALLY AVAILABLE OR GENERAL AVAILABILITY.—The terms ''generally available'' or ''general availability'' mean—

(A) in the case of computer hardware or computer software (including encryption products), computer hardware, or computer software that is—

(i) distributed via the Internet;

(ii) widely offered for sale, license, or transfer (without regard to whether it is offered for consideration), including over-the-counter retail sales, mail order transactions, telephone order transactions, electronic distribution, or sale on approval;

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

(iv) assembled from computer hardware or computer software components that are generally available;

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

(i) supply certain installation parameters needed by the computer hardware or computer software to function properly with the computer system of the user or purchaser; or

(ii) select from among options contained in the computer hardware or computer software; and

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

(6) KEY.—The term ''key'' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire communications, electronic communications, or electronically stored information, that has been encrypted.

(7) LICENSE EXCEPTION.—The term ''license exception'' means an authorization by the Bureau of

Export Administration of the Department of Commerce that allows the export or re-export, under stated conditions, of items subject to the Export Administration Regulations that otherwise would require a license.

(8) NIST.—The term ''NIST'' means the National Institute of Standards and Technology in the Department of Commerce.

(9) ON-LINE MERCHANT.—The term ''on-line merchant'' means either a person or a company or other entity engaged in commerce that, as part of its business, uses electronic means to conduct commercial transactions in goods (including, but not limited to, software and all other forms of digital content) or services, whether delivered in tangible or electronic form.

(10) PERSON.—The term ''person'' has the meaning given the term in section 2510(1) of title 1, United States Code.

(11) PUBLICLY AVAILABLE OR PUBLIC AVAILABILITY.—The terms ''publicly available'' or ''public availability'' mean—

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

(B) technology and software that are already published or will be published, arise during, or result from fundamental research, are educational, or are included in certain patent applications.

(12) RECOVERABLE PRODUCT.—The term ''recoverable product'' means an encryption product that—

(A) incorporates an operator-controlled management interface enabling real-time access to specified network traffic prior to encryption, or after decryption, at a designated access point under the control of the network owner or operator (utilizing a protocol such as IPSec);

(B) permits access to data prior to encryption, or after decryption, at a server under the control of a network owner or operator (utilizing a protocol such as SSL, TLS, or Kerberos);

(C) includes a key or data recovery system which, when activated, enables a system administrator or user to recover plaintext or keys to decrypt data transmitted or stored in encrypted form; or

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

(13) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

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

(15) STRATEGIC PARTNERS.—The term ''strategic partners'' means 2 or more entities that—

(A) have a business need to share the proprietary information of 1 or more United States companies; and

(B) are contractually bound to one another; or

(C) have an established pattern on continuing or recurring contractual relations.

(16) TECHNICAL ASSISTANCE.—The term ''technical assistance'' includes assistance such as instructions, skills training, working knowledge, and consulting services, and may involve transfer of technical data.

(17) TECHNICAL DATA.—The term ''technical data'' may include data such as blueprints, plans,

diagrams, models, formulae, tables, engineering designs and specifications, manuals, and instructions written or recorded on other media or devices such as disk, tape, or read-only memories.

(18) TECHNICAL REVIEW.—The term ''technical review'' means a review by the Secretary of an encryption product, based on information about a product's encryption capabilities supplied by the manufacturer, that an encryption product works as represented.

(19) UNITED STATES PERSON.—The term ''United States person'' means any—

(A) United States citizen; or

(B) legal entity that—

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

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

(20) UNITED STATES SUBSIDIARY.—The term ''United States subsidiary'' means—

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

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

(i) a United States company or entity beneficially owns or controls (whether directly or indirectly) 25 percent or more of the voting securities of the foreign subsidiary or entity, if no other person owns or controls (whether directly or indirectly) an equal or larger percentage;

(ii) the foreign subsidiary or entity is operated by a United States company or entity pursuant to the provisions of an exclusive management contract;

(iii) the majority of the members of the Board of Directors of the foreign subsidiary or entity also are members of the comparable governing body of the United States company or entity;

(iv) a United States company or entity has the authority to appoint the majority of the members of the Board of Directors of the foreign subsidiary; or

(v) a United States company or entity has the authority to appoint the Chief Op-

erating officer of the foreign subsidiary or entity.

TITLE I—DOMESTIC ENCRYPTION PROVISIONS

SEC. 101. DEVELOPMENT AND DEPLOYMENT OF ENCRYPTION A VOLUNTARY PRIVATE SECTOR ACTIVITY.

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

(b) LIMITATION ON REGULATION.—Neither the Federal Government nor a State may establish any conditions, ties, or links between encryption products, standards, and services used for confidentiality, and those used for authenticity or integrity purposes.

SEC. 102. SALE AND USE OF ENCRYPTION LAWFUL.

Except as otherwise provided by this Act, it is lawful for any person within any State, and for any United States person in a foreign country, to develop, manufacture, sell, distribute, import, or use any encryption product, regardless of the encryption algorithm selected, encryption length chosen, existence of key recovery, or

other plaintext access capability, or implementation or medium used.

SEC. 103. MANDATORY GOVERNMENT ACCESS TO PLAINTEXT PROHIBITED.

(a) IN GENERAL.—No department, agency, or instrumentality of the United States or of any State may—

(1) require that;

(2) set standards for;

(3) condition any approval on;

(4) create incentives for; or

(5) tie any benefit to,

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

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

(B) given to any other person (including a department, agency, or instrumentality of the United States or an entity in the private sector that may be certified or approved by the United States or a State); or

(C) retained by the owner or user of an encryption key or any other person, other than for encryption products for the use of the

United States Government or a State government.

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

TITLE II—GOVERNMENT PROCUREMENT

SEC. 201. POLICY.

It is the policy of the United States—

(1) to permit the public to interact with government through commercial networks and infrastructure; and

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

SEC. 202. FEDERAL PURCHASES OF ENCRYPTION PRODUCTS.

(a) IN GENERAL.—Any department, agency, or instrumentality of the United States may purchase encryption products for use by officers and employees of

the United States to the extent and in the manner authorized by law.

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

(c) CITIZENS NOT REQUIRED TO PURCHASE SPECIFIED PRODUCT.—No department, agency, or instrumentality of the United States, nor any department, agency, or political subdivision of a State, may require any person in the private sector to use any particular encryption product or methodology, including products with a decryption key, access to a key, key recovery information, or any other plaintext access capability, to communicate with, or transact business with, the government.

TITLE III—ADVANCED ENCRYPTION STANDARD

SEC. 301. DEADLINE FOR FINAL SELECTION OF ALGORITHM OR ALGORITHMS BY NIST.

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

(1) establishing performance requirements,

(2) setting procedures for submitting, testing, evaluating, and judging proposals; and

(3) finally selecting one or more new private sector-developed encryption algorithms.

(b) DEADLINE.—Notwithstanding subsection (a), NIST shall make a final selection of one or more new private sector-developed encryption algorithms by January 1, 2002.

SEC. 302. COMMERCE DEPARTMENT ENCRYPTION STANDARDS AND EXPORTS AUTHORITY RESTRICTED.

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

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

(b) EXPORT AUTHORITY.—Except as otherwise provided in this Act, the Secretary of Commerce may not promulgate or enforce any regulation, adopt any standard, or carry out any policy relating to encryption that has the effect of imposing government-designed encryption standards on the private sector by restricting the export of encryption products.

TITLE IV—IMPROVEMENT OF GOVERNMENTAL TECHNOLOGICAL CAPABILITY

SEC. 401. INFORMATION TECHNOLOGY LABORATORY.

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

(1) by striking ''and'' at the end of paragraph (4);

(2) by striking ''policy.'' in paragraph (5) and inserting ''policy;''; and

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

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

''(7) to research and develop new and emerging techniques and technologies to facilitate lawful access to communications and electronic information;

''(8) to research and develop methods to detect and prevent unwanted intrusions into commercial computer networks, particularly those interconnected with computer systems of the United States government;

''(9) to provide assistance in responding to information security threats and vulnerabilities at the request of other departments, agencies, and instrumentalities of the United States and State governments; and

''(10) to facilitate the development and adoption of the best information security practices by departments, agencies, and instrumentalities of the United States, the States, and the private sector.''.

SEC. 402. ADVISORY BOARD ON COMPUTER SYSTEM SECURITY AND PRIVACY.

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

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

(2) by inserting after paragraph (1) the following:

''(2) to provide a forum for communication and coordination between industry and the Federal Government regarding information security issues;

''(3) to foster the aggregation and dissemination of general, nonproprietary, and non-confidential developments in important information security technologies, including encryption, by regularly reporting that information to appropriate Federal agencies to keep law enforcement and national security agencies abreast of emerging technologies so they are able effectively to meet their responsibilities;''.

SEC. 403. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to such departments and agencies as may be appropriate such sums as may be necessary to ensure that United States law enforcement agencies and agencies responsible for national security are able to complete any missions or goals authorized in law regardless of technological advancements in encryption and digital technology.

TITLE V—EXPORT OF ENCRYPTION PRODUCTS.

SEC. 501. COMMERCIAL ENCRYPTION PRODUCTS.

(a) IN GENERAL.—This title applies to all encryption products, without regard to the encryption algorithm selected, encryption key chosen, exclusion of plaintext access

capability, or implementation or medium used, except those encryption products specifically designed or modified for military use (including command, control, and intelligence applications).

(b) AUTHORITY OF SECRETARY OF COMMERCE.—Subject to the other provisions of this title, and notwithstanding any other provision of law, the Secretary of Commerce has exclusive authority to control the exportation of encryption products described in subsection (a). In exercising that authority, the Secretary shall consult with the Secretary of State and the Secretary of Defense.

SEC. 502. PRESIDENTIAL AUTHORITY.

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

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

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

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

(i) provide support for acts of terrorism; or

(ii) pose an immediate threat to national security; or

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

(b) SPECIAL DENIALS FOR SPECIFIC REASONS.—The Secretary of Commerce shall prohibit the exportation of particular encryption products to an individual or organization in a foreign country identified by the Secretary if the Secretary determines that there is substantial evidence that the encryption products may be used or modified for military or terrorist use, including acts against the national security of, public safety of, or the integrity of the transportation, communications, or other essential systems of interstate commerce in, the United States.

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

SEC. 503. EXPORTATION OF ENCRYPTION PRODUCTS WITH NOT MORE THAN 64-BIT KEY LENGTH.

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

SEC. 504. EXPORTABILITY OF CERTAIN ENCRYPTION PRODUCTS UNDER A LICENSE EXCEPTION.

(a) LICENSE EXCEPTIONS.—Except as otherwise provided under this title, the export or re-export of the following products shall be exportable under license exception:

(1) Recoverable products.

(2) Encryption products to legitimate and responsible entities or organizations and their strategic partners, including—

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

(B) firms subject to a governmental regulatory scheme;

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

(D) firms or organizations that are required by law to maintain plaintext records of communications or otherwise maintain such

records as part of their normal business practice;

(E) firms or organizations that are audited annually under widely accepted accounting principles;

(F) strategic partners of United States companies; and

(G) on-line merchants who use encryption products to support electronic commerce, including protecting commercial transactions as well as non-public information exchange necessary to support such transactions.

(3) Encryption products sold or licensed to foreign governments that are members of the North Atlantic Treaty Organization, Organization for Economic Cooperation and Development, and Association of Southeast Asian Nations.

(4) Any computer hardware or computer software that does not itself provide encryption capabilities, but that incorporates or employs in any form interface mechanisms for interaction with other computer hardware and computer software, including encryption products.

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

encryption products, or products incorporating, enabling, or employing encryption products, if such products are exportable under this title.

(b) LICENSE EXCEPTION PROCESSING PERIOD INCLUDING ONE-TIME TECHNICAL REVIEW.—Encryption products and related computer services shall be made eligible for a license exception after a one-time technical review. Exporters' requests for license exceptions, including the one-time technical review, must be processed within 15 working days from receipt of a request. If the exporter is not contacted within this 15-day processing period, the exporter's request for a license exception will be deemed granted, and the exporter may export the encryption products or related computer services under the license exception.

SEC. 505. EXPORTABILITY OF ENCRYPTION PRODUCTS EMPLOYING A KEY LENGTH GREATER THAN 64-BITS.

(a) EXPORT RELIEF FOR ENCRYPTION PRODUCTS.—Encryption products, or products that incorporate or employ in any form, implementation, or medium an encryption product, are exportable under a license exception if—

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

(2) the Encryption Export Advisory Board described in subsection (b) determines, and the Secretary agrees, that the product or service is—

(A) generally available;

(B) publicly available; or

(C) an encryption product utilizing the same or greater key length or otherwise providing comparable security is, or will be within the next 12 months generally or widely available outside the United States from a foreign supplier.

(b) BOARD DETERMINATION OF EXPORTABILITY.—

(1) ENCRYPTION EXPORT ADVISORY BOARD.—There is hereby established an Encryption Export Advisory Board comprised of—

(A) a Chairman, who shall be the Under Secretary of Commerce for Export Administration;

(B) 7 individuals appointed by the President, as follows—

(i) 1 representative from the National Security Agency;

(ii) 1 representative from the Central Intelligence Agency;

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

(iv) 4 representatives from the private sector who have expertise in the development, operation, or marketing of information technology products; and

(C) 4 representatives from the private sector who have expertise in the development, operation, or marketing of information technology products appointed by the Congress, as follows—

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

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

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

(iv) 1 representative appointed by the Minority Leader of the House of Representatives.

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

days with respect to general availability, public availability, or foreign availability whenever an application for a license exception based on general availability, public availability, or foreign availability has been submitted to the Secretary.

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

(4) ACTION BY THE SECRETARY.—The Board shall make recommendations to the Secretary. The Secretary shall specifically approve or disapprove of each finding of availability within 30 days of receiving the recommendation and shall notify the Board and publish the finding in the Federal Register. The Secretary shall explain in detail the reasons for any disapproval, including why and how continued controls will be effective in achieving their purpose and the amount of lost sales and loss in market share of United States encryption products.

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

be subject to judicial review under the Administrative Procedure Act (5 U.S.C. 551 et seq.).

(6) PRESIDENTIAL OVERRIDE.—The Board shall report to the President within 30 days after each meeting. The President may override any Board determination of exportability and control the export and re-export of specified encryption products to specific countries or individuals if he determines that such exports or re-exports would harm United States national security, including United States capabilities in fighting drug trafficking, terrorism, or espionage. If the President overrides a Board determination of exportability and decides to control the export or re-export of any encryption product, the President must inform the Board and Congress and detail the reasons for such controls within 30 days of the determination. The action of the president under this paragraph is not subject to judicial review.

(c) RELY ON DETERMINATION OF BOARD.—The manufacturer or exporter of an encryption product or a product incorporating or employing an encryption product may rely upon the Board's determination that the product is generally available or publicly available or if a comparable foreign encryption product is available, and shall

not be held liable or responsible or subject to sanctions for any export of such products under the license exception.

(d) LICENSE EXCEPTION PROCESSING PERIOD INCLUDING ONE-TIME TECHNICAL REVIEW.—Encryption products and related computer services shall be made eligible for a license exception after a one-time technical review. Exporters' requests for license exceptions, including the one-time technical review, must be processed within 15 working days from receipt of a request. If the exporter is not contacted within this 15-day processing period, the exporter's request for a license exception will be deemed granted, and the exporter may export the encryption products or related computer services under the license exception.

(e) GRANDFATHERING OF PRIOR DETERMINATIONS.—Any determination by the Secretary prior to enactment of this Act that an encryption product with greater than a 64-bit key length, or product incorporating or employing such an encryption product, and related services, is eligible for export and re-export either without a license or under a license, a license exception, or an encryption licensing arrangement will remain in effect after passage of this Act.

SEC. 506. EXPORTABILITY OF ENCRYPTION PRODUCTS EMPLOYING AES OR ITS EQUIVALENT.

Upon adoption of the AES, but not later than January 1, 2002, the Secretary may no longer impose United States encryption export controls on encryption products if the encryption algorithm and key length employed were incorporated in the AES, or have an equivalent strength, and such product shall be exportable without the need for an export license or license exception, and without restrictions other than those permitted under this Act.

SEC. 507. ELIMINATION OF REPORTING REQUIREMENTS.

The Secretary may not impose any reporting requirements on any encryption product not subject to United States export controls or exported under a license exception.

○