

105TH CONGRESS  
1ST SESSION

# S. 909

To encourage and facilitate the creation of secure public networks for communication, commerce, education, medicine, and government.

---

IN THE SENATE OF THE UNITED STATES

JUNE 16, 1997

Mr. MCCAIN (for himself, Mr. KERREY, and Mr. HOLLINGS) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

## A BILL

To encourage and facilitate the creation of secure public networks for communication, commerce, education, medicine, and government.

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

3 **SEC. 1. SHORT TITLE.**

4 This Act may be cited as the “Secure Public Net-  
5 works Act”.

6 **SEC. 2. DECLARATION OF POLICY.**

7 It is the policy of the United States to encourage and  
8 facilitate the creation of secure public networks for com-

1 munication, commerce, education, research, medicine and  
2 government.

3       **TITLE I—DOMESTIC USES OF**  
4                   **ENCRYPTION**

5       **SEC. 101. LAWFUL USE OF ENCRYPTION.**

6           Except as otherwise provided by this Act or otherwise  
7 provided by law, it shall be lawful for any person within  
8 any State to use any encryption, regardless of encryption  
9 algorithm selected, encryption key length chosen, or imple-  
10 mentation technique or medium used.

11       **SEC. 102. PROHIBITION ON MANDATORY THIRD PARTY ES-**  
12                   **CROW OF KEYS USED FOR ENCRYPTION OF**  
13                   **CERTAIN COMMUNICATIONS.**

14           Neither the Federal Government nor a State may re-  
15 quire the escrow of an encryption key with a third party  
16 in the case of an encryption key used solely to encrypt  
17 communications between private persons within the Unit-  
18 ed States.

19       **SEC. 103. VOLUNTARY PRIVATE SECTOR PARTICIPATION IN**  
20                   **KEY MANAGEMENT STRUCTURE.**

21           The participation of the private persons in the key  
22 management infrastructure enabled by this Act is vol-  
23 untary.

1 **SEC. 104. UNLAWFUL USE OF ENCRYPTION.**

2       Whoever knowingly encrypts data or communications  
3 in furtherance of the commission of a criminal offense for  
4 which the person may be prosecuted in a court of com-  
5 petent jurisdiction and may be sentenced to a term of im-  
6 prisonment of more than one year shall, in addition to any  
7 penalties for the underlying criminal offense, be fined  
8 under title 18, United States Code, or imprisoned not  
9 more than five years, or both, for a first conviction or  
10 fined under title 18, United States Code, or imprisoned  
11 not more than ten years, or both, for a second or subse-  
12 quent conviction. The mere use of encryption shall not  
13 constitute probable cause to believe that a crime is being  
14 or has been committed.

15 **SEC. 105. PRIVACY PROTECTION.**

16       (a) IN GENERAL.—It shall be unlawful for any per-  
17 son to intentionally—

18           (1) obtain or use recovery information without  
19 lawful authority for the purpose of decrypting data  
20 or communications;

21           (2) exceed lawful authority in decrypting data  
22 or communications;

23           (3) break the encryption code of another person  
24 without lawful authority for the purpose of violating  
25 the privacy, security or property rights of that per-  
26 son;

1 (4) intercept on a public communications net-  
2 work without lawful authority the intellectual prop-  
3 erty of another person for the purpose of violating  
4 the intellectual property rights of that person;

5 (5) impersonate another person for the purpose  
6 of obtaining recovery information of that person  
7 without lawful authority;

8 (6) issue a key to another person in furtherance  
9 of a crime;

10 (7) disclose recovery information in violation of  
11 a provision of this Act; or

12 (8) publicly disclose without lawful authority  
13 the plaintext of information that was decrypted  
14 using recovery information obtained with or without  
15 lawful authority.

16 (b) CRIMINAL PENALTY.—Any person who violates  
17 this section shall be fined under title 18, United States  
18 Code, or imprisoned not more than five years, or both.

19 **SEC. 106. ACCESS TO ENCRYPTED MESSAGES BY GOVERN-**  
20 **MENT ENTITIES.**

21 (1) EFFECT ON EXISTING AUTHORITIES.—Nothing  
22 in this section authorizes a government entity to obtain  
23 recovery information from any key recovery agent unless  
24 the government entity has lawful authority to obtain com-

1 munications or electronically stored information apart  
2 from this Act.

3 (2) **LAWFUL PURPOSES.**—A key recovery agent,  
4 whether or not registered by the Secretary under this Act,  
5 shall disclose recovery information:

6 (a) To a government entity if that entity is au-  
7 thorized to use the recovery information to deter-  
8 mine the plaintext of information it has obtained or  
9 is obtaining pursuant to a duly-authorized warrant  
10 or court order, a subpoena authorized by Federal or  
11 State statute or rule, a certification issued by the  
12 Attorney General under the Foreign Intelligence  
13 Surveillance Act, or other lawful authority; or

14 (b) To a government entity to permit that en-  
15 tity to comply with a request from a foreign govern-  
16 ment that the entity is authorized to execute under  
17 United States law.

18 (3) **PROCEDURES.**—A key recovery agent, whether or  
19 not registered by the Secretary under this Act, shall dis-  
20 close recovery information to a Federal or State govern-  
21 ment entity, to permit it to achieve the lawful purposes  
22 specified in subsection (2) of this section upon the receipt  
23 of a subpoena described in subsection (4) which is based  
24 upon a duly authorized warrant or court order authorizing  
25 interception of wire communications or electronic commu-

1 nications authorized under chapter 119 or title 18, United  
 2 States code, or applicable State statute, or authorizing ac-  
 3 cess to stored wire and electronic communications and  
 4 transactional records under chapter 121 of title 18, Unit-  
 5 ed States Code, or applicable State statute; a subpoena  
 6 authorized by or based on authority established by Federal  
 7 or State law, statute, precedent or rule; a warrant or court  
 8 order or certification issued by the Attorney General au-  
 9 thorized under the Foreign Intelligence Surveillance Act,  
 10 50 United State Code 1801 et seq. or other lawful author-  
 11 ity, and directing such key recovery agent to provide as-  
 12 sistance.

13 (4) SUBPOENA.—The Attorney General shall by rule  
 14 prescribe the form of a uniform subpoena and identify the  
 15 necessary endorsements for such a subpoena to ensure the  
 16 lawful disclosure of key recovery information to a Federal  
 17 or State government entity by a Key Recovery Agent au-  
 18 thorized under subsection (2) of this section.

19 (5) AUDITS.—The Attorney General shall establish  
 20 periodic audits of subpoenas issued under this section to  
 21 ensure that subpoenas issued are pursuant to lawful au-  
 22 thority. In the event an audit finds a subpoena issued  
 23 without lawful authority, the Attorney General shall en-  
 24 sure that necessary disciplinary, investigatory, and pros-  
 25 ecutorial steps are taken.

1 **SEC. 107. CIVIL RECOVERY.**

2 (a) IN GENERAL.—Except as otherwise provided in  
3 this Act, any person described in subsection (b) may in  
4 a civil action recover from the United States Government  
5 the actual damages suffered by the person as result of a  
6 violation described in that subsection, a reasonable attor-  
7 ney's fee, and other litigation costs reasonably incurred.

8 (b) COVERED PERSONS.—Subsection (a) applies to  
9 any person—

10 (1) whose recovery information is knowingly ob-  
11 tained without lawful authority by an agent of the  
12 United States Government from a key recovery  
13 agent or certificate authority registered under this  
14 Act;

15 (2) whose recovery information is obtained by  
16 an agent of the United States Government with law-  
17 ful authority from a key recovery agent or certificate  
18 authority registered under this Act and is knowingly  
19 used or disclosed without lawful authority; or

20 (3) whose recovery information is obtained by  
21 an agent of the United States Government with law-  
22 ful authority from a key recovery agent or certificate  
23 authority registered under this Act and is used to  
24 publicly disclose decrypted information without law-  
25 ful authority.

1 (c) LIMITATION.—A civil action under this section  
2 shall be commenced not later than two years after the date  
3 on which the claimant first discovers the violation.

4 **SEC. 108. USE AND HANDLING OF DECRYPTED INFORMA-**  
5 **TION.**

6 (a) AUTHORIZED USE OF DECRYPTED INFORMA-  
7 TION.—A government entity to which recovery informa-  
8 tion is released in accordance with this Act may use the  
9 plaintext information obtained with the recovery informa-  
10 tion only for lawful purposes.

11 (b) HANDLING OF DECRYPTED INFORMATION.—  
12 Upon completion of the use of plaintext information ob-  
13 tained with recovery information released under this Act,  
14 the government entity concerned shall handle and protect  
15 the privacy of the plaintext information in a manner con-  
16 sistent with applicable Federal or State statute, law or  
17 rule.

18 **SEC. 109. USE AND DESTRUCTION OR RETURN OF RECOV-**  
19 **ERY INFORMATION.**

20 (a) AUTHORIZED USE OF RECOVERY INFORMA-  
21 TION.—

22 (1) IN GENERAL.—A government entity to  
23 which recovery information is released under this  
24 Act may use the recovery information only for lawful  
25 purposes.



(2) LIMITATION.—A government entity may not use recovery information obtained under this Act to determine the plaintext of any wire communication or electronic communication or of any stored electronic information unless it has lawful authority to determine the plaintext under provisions of law other than this Act.

(b) RETURN OR DESTRUCTION OF INFORMATION.—

Upon completion of the use of recovery information obtained under this Act, the government entity concerned shall unless otherwise required by law destroy the information or return the information to the key recovery agent and shall make a record documenting such destruction or return.

(c) NOTICE.—When a government entity destroys a key pursuant to this section, the government entity shall notify the key recovery agent of such destruction.

18 SEC. 110. DISCLOSURE OR RELEASE OF RECOVERY INFOR-  
19 MATION.

20 Except as otherwise authorized by this Act, a key re-  
21 covery agent or other person may not disclose to any per-  
22 son the facts or circumstances of any release of recovery  
23 information pursuant to section 106, or of any requests  
24 therefor, unless under an order by a Federal court of com-  
25 petent jurisdiction.

1 **SEC. 111. NOTIFICATION TO RECIPIENTS OF RECOVERY IN-**  
2 **FORMATION.**

3 A key recovery agent or certificate authority, whether  
4 or not registered under this Act, who discloses recovery  
5 information shall—

6 (1) notify the recipient that recovery informa-  
7 tion is being disclosed; and

8 (2) specify which part of the information dis-  
9 closed is recovery information.

10 **TITLE II—GOVERNMENT**  
11 **PROCUREMENT**

12 **SEC. 201. POLICY.**

13 It is the policy of the United States Government to  
14 facilitate the creation of secure networks that permit the  
15 public to interact with the government through networks  
16 which protect privacy, the integrity of information, rights  
17 in intellectual property, and the personal security of net-  
18 work users.

19 **SEC. 202. FEDERAL PURCHASES OF ENCRYPTION PROD-**  
20 **UCTS.**

21 Any encryption product purchased or otherwise pro-  
22 cured by the United States Government for use in secure  
23 government networks shall be based on a qualified system  
24 of key recovery.

1 **SEC. 203. ENCRYPTION PRODUCT PURCHASED WITH FED-**  
2 **ERAL FUNDS.**

3 Any encryption product purchased directly with Fed-  
4 eral funds for use in secure public networks shall be based  
5 on a qualified system of key recovery.

6 **SEC. 204. UNITED STATES GOVERNMENT NETWORKS.**

7 Any communications network established by the  
8 United States Government after the date of enactment of  
9 this Act which uses encryption products as part of the net-  
10 work shall use encryption products based on a qualified  
11 system of key recovery.

12 **SEC. 205. NETWORKS ESTABLISHED WITH FEDERAL FUNDS.**

13 Any encrypted communications network established  
14 after the date of enactment of this Act with the use of  
15 Federal funds shall use encryption products based on a  
16 qualified system of key recovery.

17 **SEC. 206. PRODUCT LABELS.**

18 An encryption product may be labeled to inform users  
19 that the product is authorized for sale to or for use in  
20 transactions and communications with the United States  
21 Government under this title.

22 **SEC. 207. NO PRIVATE MANDATE.**

23 The United States Government may not mandate the  
24 use of encryption standards for the private sector other  
25 than for use with computer systems, networks or other

1 systems of the United States Government, or systems or  
 2 networks created using Federal funds.

3 **SEC. 208. TRANSITION RULES.**

4 The Secretary may though rule provide for the or-  
 5 derly implementation of this section and the effective use  
 6 of secure public networks.

7 **SEC. 209. INTEROPERABILITY.**

8 In establishing the criteria for a qualified system of  
 9 key recovery, the Secretary shall consider providing for the  
 10 interoperability of key recovery products procured under  
 11 this section with non-key recovery products to ensure that  
 12 citizens have secure network access to their government.

13 **TITLE III—EXPORT OF**  
 14 **ENCRYPTION**

15 **SEC. 301. THE DEPARTMENT OF COMMERCE.**

16 The Secretary of Commerce in consultation with  
 17 other relevant executive branch agencies shall have juris-  
 18 diction over the export of commercial encryption products.  
 19 The Secretary shall have the sole duty to issue export li-  
 20 censes on commercial encryption products.

21 **SEC. 302. LICENSE EXCEPTION NON-KEY RECOVERY.**

22 Exports of encryption products up to and including  
 23 56 bit DES or equivalent strength shall be exportable  
 24 under a license exception, following a one time receive,  
 25 provided the encryption product being exported—

- 1 (1) is otherwise qualified for export;
- 2 (2) is otherwise legal;
- 3 (3) does not violate U.S. law;
- 4 (4) does not violate the intellectual property
- 5 rights of another; and
- 6 (a) the recipient individual is otherwise
- 7 qualified to review such encryption product; and
- 8 (b) the country to which the encryption
- 9 product is to be exported is otherwise qualified
- 10 to receive the encryption product.

11 The Secretary shall complete a license exception review  
12 under this section within ten working days of a properly  
13 filed license exception request.

14 **SEC. 303. PRESIDENTIAL ORDER.**

15 The President may by executive order increase the  
16 encryption strength for encryption products which may be  
17 exported under section 302 of this Act. The encryption  
18 strength for encryption products which may be exported  
19 under section 302 of this Act shall be reviewed by the  
20 President on an annual basis. Consistent with other provi-  
21 sions of this Title and Section 901 of this Act, the Presi-  
22 dent shall take such action as necessary to increase the  
23 encryption strength for encryption products which may be  
24 exported if similar products are determined by the Presi-  
25 dent to be widely available for export from other Nations.

1 **SEC. 304. LICENSE EXCEPTION FOR KEY RECOVERY.**

2 Encryption products may be exported under a license  
3 exception, following a one time review without regard to  
4 the encryption algorithm selected or encryption key length  
5 chosen when such encryption product is based on a quali-  
6 fied system of key recovery, provided, the encryption prod-  
7 uct being exported—

8 (1) is otherwise qualified for export;

9 (2) is otherwise legal;

10 (3) does not violate U.S. law;

11 (4) does not violate the intellectual property  
12 right of another; and

13 (a) the recipient individual is otherwise  
14 qualified to receive such product; and

15 (b) the country to which the encryption  
16 product is to be exported is otherwise qualified  
17 to receive the encryption product.

18 The Secretary shall describe the elements of a qualified  
19 system of key recovery and the procedures for establishing  
20 compliance with those elements. The Secretary shall com-  
21 plete a license exception review under this section within  
22 ten working days of a properly filed license exception re-  
23 quest.

24 **SEC. 305. EXPEDITED REVIEW FOR CERTAIN INSTITUTIONS.**

25 The Secretary in consultation with other relevant ex-  
26 ecutive branch agencies shall establish a procedure for ex-

1 pedited review of export license applications involving  
2 encryption products for use by qualified Banks, Financial  
3 Institutions and Health Care Providers, subsidiaries of  
4 U.S. Owned and controlled companies or other users au-  
5 thorized by the Secretary.

6 **SEC. 306. PROHIBITED EXPORTS.**

7       The export of any encryption product shall be prohib-  
8 ited when the Secretary in consultation with other agen-  
9 cies finds evidence that the encryption product to be ex-  
10 ported would be used in acts against the national security,  
11 the public safety, transportation systems, communications  
12 networks, financial institutions or other essential systems  
13 of interstate commerce; diverted to a military, terrorist or  
14 criminal use; or re-exported without authorization. The  
15 Secretary's decision on the grounds for a prohibition  
16 under his section shall not be subject to judicial review.

17 **SEC. 307. LICENSE REVIEW.**

18       In evaluating applications for export licenses for  
19 encryption products not based on a qualified key recovery  
20 system, in strengths above the level described in Section  
21 302, the following factors shall be among those considered  
22 by the Secretary:

- 23           (1) whether an encryption product is generally  
24       available and is designed for installation without al-  
25       teration by purchaser;

1           (2) whether the encryption product is generally  
2           available in the country to which the encryption  
3           product would be exported;

4           (3) whether encryption products offering com-  
5           parable security and level of encryption is available  
6           in the country to which the encryption product  
7           would be exported; or

8           (4) whether the encryption product will be im-  
9           minently available in the country to which the prod-  
10          uct would be exported.

11 The Secretary shall complete a license review under this  
12 section within thirty working days of a properly filed li-  
13 cense request. The Secretary's decision on the grounds for  
14 the grant or denial of license shall not be subject to judi-  
15 cial review.

16 **SEC. 308. CRIMINAL PENALTIES.**

17       Any person who exports an encryption product in vio-  
18 lation of this Title shall be fined under Title 18, United  
19 States Code or imprisoned for not more than five years.

20                   **TITLE IV—VOLUNTARY**  
21                   **REGISTRATION SYSTEM**

22 **SEC. 401. VOLUNTARY USE OF CERTIFICATE AUTHORITIES**  
23                   **AND KEY RECOVERY AGENTS.**

24       Except as provided in Title II of this Act, nothing  
25 in this Act may be construed to require a person, in com-



1 munications between private persons within the United  
2 States, to—

3           (1) use an encryption product with a key recov-  
4       ery feature;

5           (2) use a public key issued by a certificate au-  
6       thority registered under this Act; or

7           (3) entrust key recovery information with a key  
8       recovery agent registered under this Act.

9 **SEC. 402. REGISTRATION OF CERTIFICATE AUTHORITIES.**

10       (a) **AUTHORITY TO REGISTER.**—The Secretary or  
11 the Secretary’s designee may register any private person,  
12 entity, government entity, or foreign government agency  
13 to act as a certificate authority if the Secretary determines  
14 that the person, entity or agency meets such standards  
15 relating to security in and performance of the activities  
16 of a certificate authority registered under this Act.

17       (b) **AUTHORIZED ACTIVITIES OF REGISTERED CER-**  
18 **TIFICATE—AUTHORITIES.**—

19           (1) A certificate authority registered under this  
20       section may issue public key certificates which may  
21       be used to verify the identity of a person engaged in  
22       encrypted communications for such purposes as au-  
23       thentication, integrity, nonrepudiation, digital signa-  
24       ture, and other similar purposes.

1           (2) A certificate authority registered under this  
2           section may issue public key certificates which may  
3           be used for encryption.

4           (3) The Secretary shall not, as a condition of  
5           registration under this Act, require any certificate  
6           authority to store with a third party information  
7           used solely for the purposes in subparagraph (b)(1)  
8           of this section.

9           (c) CONDITION MODIFICATION AND REVOCATION OF  
10          REGISTRATION.—The Secretary may condition, modify or  
11          revoke the registration of a certificate authority under this  
12          section if the Secretary determines that the certificate au-  
13          thority has violated any provision of this Act, or any regu-  
14          lations thereunder, or for any other reason specified in  
15          such regulations.

16          (d) REGULATIONS.—

17               (1) REQUIREMENT.—The Secretary in consulta-  
18               tion with other relevant executive branch agencies  
19               shall prescribe regulations relating to certificate au-  
20               thorities registered under this section. The regula-  
21               tions shall be consistent with the purposes of this  
22               Act.

23               (2) ELEMENTS.—The regulations prescribed  
24               under this subsection shall—

1 (A) establish requirements relating to the  
2 practices of certificate authorities, including the  
3 basis for the modification or revocation of reg-  
4 istration under subsection (c);

5 (B) specify reasonable requirements for  
6 public key certificates issued by certificate au-  
7 thorities which requirements shall meet gen-  
8 erally accepted standards for such certificates;

9 (C) specify reasonable requirements for  
10 record keeping by certificate authorities;

11 (D) specify reasonable requirements for  
12 the content, form, and sources of information in  
13 disclosure records of certificate authorities, in-  
14 cluding the updating and timeliness of such in-  
15 formation, and for other practices and policies  
16 relating to such disclosure records; and

17 (E) otherwise give effect to and implement  
18 the provisions of this Act relating to certificate  
19 authorities.

20 **SEC. 403. REGISTRATION OF KEY RECOVERY AGENTS.**

21 (a) **AUTHORITY TO REGISTER.**—The Secretary or  
22 the Secretary’s designee may register a private person, en-  
23 tity, or government entity to act as a key recovery agent  
24 if the Secretary determines that the person or entity pos-

1 sesses the capability, competency, trustworthiness, and re-  
 2 sources to

3 (1) safeguard sensitive information;

4 (2) carry out the responsibilities set forth in  
 5 subsection (b); and

6 (3) comply with such regulations relating to the  
 7 practices of key recovery agents as the Secretary  
 8 shall prescribe.

9 (b) RESPONSIBILITIES OF KEY RECOVERY  
 10 AGENTS.—A key recovery agent registered under sub-  
 11 section (a) shall, consistent with any regulations pre-  
 12 scribed under subsection (a), establish procedures and  
 13 take other appropriate steps to—

14 (1) ensure the confidentiality, integrity, avail-  
 15 ability, and timely release of recovery information  
 16 held by the key recovery agent;

17 (2) protect the confidentiality of the identity of  
 18 the person or persons for whom the key recovery  
 19 agent holds recovery information;

20 (3) protect the confidentiality of lawful requests  
 21 for recovery information, including the identity of  
 22 the individual or government entity requesting recov-  
 23 ery information and information concerning access  
 24 to and use of recovery information by the individual  
 25 or entity; and

1           (4) carry to the responsibilities of key recovery  
2       agents set forth in this Act and the regulations  
3       thereunder.

4       (c) CONDITION, MODIFICATION OR REVOCATION OF  
5   REGISTRATION.—The Secretary may condition, modify or  
6   revoke the registration of a key recovery agent under this  
7   section if the Secretary determines that the key recovery  
8   agent has violated any provision of this Act, or any regula-  
9   tions thereunder, or for any other reason specified in such  
10   regulations.

11       (d) REGULATIONS.—The Secretary in consultation  
12   with other relevant executive branch agencies shall pre-  
13   scribe regulations relating to key recovery agents reg-  
14   istered under this section. The regulations shall be consist-  
15   ent with the purposes of this Act.

16   **SEC. 404. DUAL REGISTRATION AS KEY RECOVERY AGENT**  
17                           **AND CERTIFICATE AUTHORITY.**

18       Nothing in this Act shall be construed to prohibit the  
19   registration as a certificate authority under section 402  
20   of a person or entity registered as a key recovery agent  
21   under section 403.

22   **SEC. 405. PUBLIC KEY CERTIFICATES FOR ENCRYPTION**  
23                           **KEYS.**

24       The Secretary or a Certificate Authority for Public  
25   Keys registered under this Act may issue to a person a

1 public key certificate that certifies a public key that can  
2 be used for encryption only if the person:

3 (1) stores with a Key Recovery Agent registered  
4 under this Act sufficient information, as specified by  
5 the Secretary in regulations, to allow timely lawful  
6 recovery of the plaintext of that person's encrypted  
7 data and communications; or

8 (2) makes other arrangements, approved by the  
9 Secretary pursuant to regulations promulgated in  
10 concurrence with the Attorney General, that assure  
11 that lawful recovery of the plaintext of encrypted  
12 data and communications can be accomplished in a  
13 timely fashion and, unless authorized under Section  
14 110 of this Act, without disclosing that data or com-  
15 munications are being recovered pursuant to a gov-  
16 ernment request.

17 **SEC. 406. DISCLOSURE OR RECOVERY INFORMATION.**

18 A key recovery agent, whether or not registered under  
19 this Act, may not disclose recovery information stored with  
20 the key recovery agent by a person unless the disclosure  
21 is—

22 (1) to the person, or an authorized agent there-  
23 of;

24 (2) with the consent of the person, including  
25 pursuant to a contract entered into with the person;

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

(A) the person who supplied the information is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(B) the person who supplied the information is afforded the opportunity to appear in the court proceeding and contest the claim of the person seeking the disclosure;

(4) pursuant to a determination by a court of competent jurisdiction that another person is lawfully entitled to hold such recovery information, including determinations arising from legal proceedings associated with the incapacity, death, or dissolution of any person; or

(5) otherwise permitted by a provision of this Act or otherwise permitted by law.

**SEC. 407. CRIMINAL ACTS.**

(a) IN GENERAL.—It shall be unlawful for—

(1) a certificate authority registered under this Act, or an officer, employee, or agent thereof, to intentionally issue a public key certificate in violation of this Act;

1           (2) any person to intentionally issue what  
2           purports to be a public key certificate issued by a  
3           certificate authority registered under this Act when  
4           such person is not a certificate authority registered  
5           under this Act;

6           (3) any person to fail to revoke what purports  
7           to be a public key certificate issued by a certificate  
8           authority registered under this Act when such per-  
9           son knows that the issuing person is not such a cer-  
10          tificate authority and have the power to revoke a  
11          public key certificate;

12          (4) any person to intentionally issue a public  
13          key certificate to a person who does not meet the re-  
14          quirements of this Act or the regulations prescribed  
15          thereunder; or

16          (5) any person to intentionally apply for or ob-  
17          tain a public key certificate under this Act knowing  
18          that the person to be identified in the public key cer-  
19          tificate does not meet the requirements of this Act  
20          or the regulations thereunder.

21          (b) CRIMINAL PENALTY.—Any person who violates  
22          this section shall be fined under title 18, United States  
23          Code, or imprisoned not more than five years, or both.



# 1 **TITLE V-LIABILITY LIMITATIONS**

## 2 **SEC. 501. NO CAUSE OF ACTION FOR COMPLYING WITH** 3 **GOVERNMENT REQUESTS.**

4       No civil or criminal liability under this Act, or under  
5 any other provision of law, shall attach to any key recovery  
6 agent, or any officer, employee, or agent thereof, or any  
7 other persons specified by the Secretary in regulations, for  
8 disclosing recovery information or providing other assist-  
9 ance to a government entity in accordance with sections  
10 106 and 406 of this Act.

## 11 **SEC. 502. COMPLIANCE DEFENSE.**

12       Compliance with the provisions of this Act and the  
13 regulations thereunder is a complete defense for certificate  
14 authorities and key recovery agents registered under this  
15 Act to any noncontractual civil action for damages based  
16 upon activities regulated by this Act.

## 17 **SEC. 503. REASONABLE CARE DEFENSE.**

18       The use by any person of a certificate authority or  
19 key recovery agent registered under this Act shall be treat-  
20 ed as evidence of reasonable care or due diligence in any  
21 judicial or administrative proceeding where the reason-  
22 ableness of the selection of the authority or agent, as the  
23 case may be, or of encryption products, is a material issue.

1 **SEC. 504. GOOD FAITH DEFENSE.**

2 A good faith reliance on legal authority requiring or  
3 authorizing access to recovery information under this Act,  
4 or any regulations thereunder, is a complete defense to  
5 any criminal action brought under this Act or any civil  
6 action.

7 **SEC. 505. LIMITATION ON FEDERAL GOVERNMENT LIABIL-**  
8 **ITY.**

9 Except as otherwise provided in this Act, the United  
10 States shall not be liable for any loss incurred by any indi-  
11 vidual or entity resulting from any violation of this Act  
12 or the performance or nonperformance of any duties under  
13 any regulation or procedure established by or under this  
14 Act, nor resulting from any action by any person who is  
15 not an official or employee of the United States.

16 **SEC. 506. CIVIL ACTION**

17 Civil action may be brought against a key recovery  
18 agent, a certificate authority or other person who violates  
19 or acts in a manner which is inconsistent with this Act.

20 **TITLE VI—INTERNATIONAL**  
21 **AGREEMENTS**

22 The President shall conduct negotiations with other  
23 countries for the purpose of mutual recognition of key re-  
24 covery agents and certificate authorities; and to safeguard  
25 privacy and prevent commercial espionage. The President  
26 shall consider a country's refusal to negotiate such mutual

1 recognition agreements when considering the participation  
 2 of the United States in any cooperation or assistance pro-  
 3 gram with that country. The President shall report to the  
 4 Congress if negotiations are not complete by the end of  
 5 1999.

## 6 **TITLE VII—GENERAL AUTHOR-** 7 **ITY AND CIVIL PENALTIES**

### 8 **SEC. 701. GENERAL AUTHORITY AND CIVIL REMEDIES.**

9 (a) **AUTHORITIES TO SECURE INFORMATION.**—To  
 10 the extent necessary or appropriate to the enforcement of  
 11 this Act or any regulation thereunder, the Secretary may  
 12 make investigations, obtain information, take sworn testi-  
 13 mony, and require reports or the keeping of records by  
 14 and make inspection of the books, records, and other  
 15 writings, premises or property of any person.

16 (b) **INVESTIGATIONS.**—

17 (1) **APPLICABLE AUTHORITIES.**—In conducting  
 18 investigations under subsection (a) the Secretary  
 19 may, to the extent necessary or appropriate to the  
 20 enforcement of this Act and subject to such require-  
 21 ments as the Attorney General shall prescribe, exer-  
 22 cise such authorities as are conferred upon the Sec-  
 23 retary by other laws of the United States.

24 (2) **ADDITIONAL AUTHORITY.**—In conducting  
 25 such investigations, the Secretary may administer

1 oaths or affirmations and may by subpoena require  
2 any person to appear and testify or to appear and  
3 produce books, records, and other writings, or both.

4 (3) WITNESSES AND DOCUMENTS.—

5 (A) IN GENERAL.—The attendance of wit-  
6 nesses and the production of documents pro-  
7 vided for in this subsection may be required in  
8 any State at any designated place.

9 (B) WITNESS FEES.—Witnesses sum-  
10 moned shall be paid the same fees and mileage  
11 that are paid to witnesses in the courts of the  
12 United States.

13 (4) ORDERS TO APPEAR.—In the case of contu-  
14 macy by, or refusal to obey a subpoena issued to any  
15 person pursuant to this subsection, the district court  
16 of the United States for the district in which such  
17 person is found, resides, or transacts business, upon  
18 application by the United States and after notice to  
19 such person, shall have jurisdiction to issue an order  
20 requiring such person to appear and give testimony  
21 before the Secretary or to appear and produce docu-  
22 ments before the Secretary, or both, and any failure  
23 to obey such order of the court may be punished by  
24 such court as a contempt thereof.

1 **SEC. 702. CIVIL PENALTIES.**

2 (a) **AUTHORITY TO IMPOSE CIVIL PENALTIES.—**

3 (1) **IN GENERAL.**—The Secretary may, after  
4 notice and an opportunity for an agency hearing on  
5 the record in accordance with sections 554 through  
6 557 of title 5, United States Code, impose a civil  
7 penalty of not more than \$100,000 for each violation  
8 of this Act or any regulation thereunder either in  
9 addition to or in lieu of any other liability or penalty  
10 which may be imposed for such violation.

11 (2) **CONSIDERATION REGARDING AMOUNT.**—In  
12 determining the amount of the penalty, the Sec-  
13 retary shall consider the risk of harm to law enforce-  
14 ment, public safety, and national security, the risk  
15 of harm to affected persons, the gross receipts of the  
16 charged party, and the willfulness of the violation.

17 (3) **LIMITATION.**—Any proceeding in which a  
18 civil penalty is sought under this subsection may not  
19 be initiated more than 5 years after the date of the  
20 violation.

21 (4) **JUDICIAL REVIEW.**—The imposition of a  
22 civil penalty under paragraph (1) shall be subject to  
23 judicial review in accordance with sections 701  
24 through 706 of title 5, United States Code.

25 (b) **RECOVERY.**—

1           (1) IN GENERAL.—A civil penalty under this  
2       section, plus interest at the currently prevailing  
3       rates from the date of the final order, may be recov-  
4       ered in an action brought by the Attorney General  
5       on behalf of the United States in the appropriate  
6       district court of the United States. In such action,  
7       the validity and appropriateness of the final order  
8       imposing the civil penalty shall not be subject to re-  
9       view.

10          (2) LIMITATION.—No action under this sub-  
11       section may be commenced more than 5 years after  
12       the order imposing the civil penalty concerned be-  
13       comes final.

14   **SEC. 703. INJUNCTIONS.**

15           The Attorney General may bring an action to  
16       enjoin any person from committing any violation of  
17       any provision of this Act or any regulation there-  
18       under.

19   **SEC. 704. JURISDICTION.**

20           The district courts of the United States shall have  
21       original jurisdiction over any action brought by the Attor-  
22       ney General under this title.

1       **TITLE VIII—RESEARCH AND**  
2                   **MONITORING**

3   **SEC. 801. INFORMATION SECURITY BOARD.**

4       (a) REQUIREMENT TO ESTABLISH.—The President  
5 shall establish an advisory board to be known as the Infor-  
6 mation Security Board (in this section referred to as the  
7 “Board”).

8       (b) MEMBERSHIP.—The Board shall be composed  
9 of—

10           (1) such number of members as the President  
11 shall appoint from among the officers or employees  
12 of the Federal Government involved in the formation  
13 of United States policy regarding secure public net-  
14 works, including United States policy on exports of  
15 products with information security features; and

16           (2) a number of members equal to the number  
17 of members under paragraph (1) appointed by the  
18 President from among individuals in the private sec-  
19 tor having an expertise in information technology or  
20 in law or policy relating to such technology.

21       (c) MEETINGS.—The Board shall meet not less often  
22 than once each year.

23       (d) DUTIES.—The Board shall review available infor-  
24 mation and make recommendations to the President and  
25 Congress on appropriate policies to ensure—

1 (1) the security of networks;

2 (2) the protection of intellectual property rights  
3 in information and products accessible through com-  
4 puter networks;

5 (3) the promotion of exports of software pro-  
6 duced in the United States;

7 (4) the national security, effective law enforce-  
8 ment, and public safety interests of the United  
9 States related to communications networks; and

10 (5) the protection of the interests of Americans  
11 in the privacy of data and communications.

12 **SEC. 802. COORDINATION OF ACTIVITIES ON SECURE PUB-**  
13 **LIC NETWORKS.**

14 In order to meet the purposes of this Act, the Presi-  
15 dent shall—

16 (1) ensure a high level of cooperation and co-  
17 ordination between the departments and agencies of  
18 the Federal Government in the formation and dis-  
19 charge of United States policy regarding secure pub-  
20 lic networks; and

21 (2) encourage cooperation and coordination be-  
22 tween the Federal Government and State and local  
23 governments in the formation and discharge of such  
24 policy.



1 **SEC. 803. NETWORK RESEARCH.**

2       It shall be a priority of the Federal Government to  
3 encourage research to facilitate the creation of secure pub-  
4 lic networks which satisfy privacy concerns, national secu-  
5 rity interests, effective law enforcement requirements, and  
6 public safety needs.

7 **SEC. 804. ANNUAL REPORT.**

8       (a) REQUIREMENT.—The National Telecommuni-  
9 cations and Information Administration shall, in consulta-  
10 tion with other Federal departments and agencies, submit  
11 to Congress and the President each year a report on devel-  
12 opments in the creation of secure public networks in the  
13 United States.

14       (b) ELEMENTS.—The report shall discuss develop-  
15 ments in encryption, authentication, identification, and se-  
16 curity on communications networks during the year pre-  
17 ceding the submittal of the report and may include rec-  
18 ommendations on improvements in United States policy  
19 to such matters.

20 **SEC. 805. NATIONAL PERFORMANCE REVIEW.**

21       The National Performance Review shall evaluate the  
22 progress of federal efforts to migrate government services  
23 and operations to secure public networks.

24 **SEC. 806. EDUCATION NETWORKS.**

25       The Department of Education, in cooperation with  
26 the National Telecommunications and Information Ad-

1 ministration and the Federal Communications Commis-  
 2 sion and the Joint Board established by the Federal Com-  
 3 munications Commission and State Departments of Edu-  
 4 cation shall evaluate technical, educational, legal and regu-  
 5 latory standards for distance learning via secure public  
 6 networks.

## 7 **TITLE IX—WAIVER AUTHORITY**

### 8 **SEC. 901. WAIVER AUTHORITY.**

9 (a) **AUTHORITY TO WAIVE.**—The President may by  
 10 executive order waive provisions of this Act, or the applica-  
 11 bility of any such provision to a person or entity, if the  
 12 President determines that the waiver is in the interests  
 13 of national security, or domestic safety and security.

14 (b) **REPORT.**—Not later than 15 days after each ex-  
 15 ercise of authority provided in subsection (a), the Presi-  
 16 dent shall submit to Congress a report on the exercise of  
 17 the authority, including the determination providing the  
 18 basis of the exercise of the authority. The report shall ex-  
 19 plain the grounds of the President’s action with specificity  
 20 and be submitted in unclassified and classified form.

## 21 **TITLE X—MISCELLANEOUS**

## 22 **PROVISIONS**

### 23 **SEC. 1001. REGULATION AND FEES.**

24 (a) **REGULATIONS.**—The Secretary shall, in consulta-  
 25 tion with the Secretary of State, the Secretary of Defense,

1 and the Attorney General and after notice to the public  
2 and opportunity for comment, prescribe any regulations  
3 necessary to carry out this Act.

4 (b) FEES.—The Secretary may provide in the regula-  
5 tions prescribed under subsection (a) for the imposition  
6 and collection of such fees as the Secretary considers ap-  
7 propriate for purposes of this Act.

8 **SEC. 1002. INTERPRETATION.**

9 Nothing contained in this Title shall be deemed to:

10 (1) pre-empt or otherwise affect the application  
11 of the Arms Export Control Act (22 U.S.C. 2751 et  
12 seq.), the Export Administration Act of 1979, as  
13 amended (50 U.S.C. app. 2401–2420), and the  
14 International Emergency Economic Powers Act (50  
15 U.S.C. 1701–1706), or regulations promulgated  
16 thereunder;

17 (2) affect intelligence activities outside the  
18 United States;

19 (3) or weaken any intellectual property protec-  
20 tion.

21 **SEC. 1003. SEVERABILITY.**

22 If any provision of this Act, or the application there-  
23 of, to any person or circumstances is held invalid, the re-  
24 mainder of this Act, and the application thereof, to other  
25 persons or circumstances shall not be affected thereby.

1 **SEC. 1004. AUTHORIZATION OF APPROPRIATIONS.**

2       There are hereby authorized to be appropriated to the  
3 Secretary of Commerce for fiscal years 1998, 1999, 2000,  
4 2001, and 2002 such sums as may be necessary to carry  
5 out responsibilities under this Act.

6 **SEC. 1005. DEFINITIONS.**

7       For purposes of this Act:

8           (1) **CERTIFICATE AUTHORITY.**—The term “cer-  
9 tificate authority” means a person trusted by one or  
10 more persons to create and assign public key certifi-  
11 cates.

12          (2) **DECRYPTION.**—The term “decryption”  
13 means the electronic retransformation of data (in-  
14 cluding communications) that has been encrypted  
15 into the data’s original form. To “decrypt” is to per-  
16 form decryption.

17          (3) **ELECTRONIC COMMUNICATION.**—The term  
18 “electronic communication” has the meaning given  
19 such term in section 2510(12) of title 18, United  
20 States Code.

21          (4) **ELECTRONIC INFORMATION.**—The term  
22 “electronic information” includes voice communica-  
23 tions, texts, messages, recordings, images, or docu-  
24 ments in any electronic, electromagnetic,  
25 photoelectronic, photooptical, or digitally encoded  
26 computer-readable form.

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

4           (6) ENCRYPTION.—The term “encryption”  
5       means the electronic transformation of data (includ-  
6       ing communications) in order to hide its information  
7       content. To “encrypt” is to perform encryption.

8           (7) ENCRYPTION PRODUCT.—The term  
9       “encryption product” includes any product, software,  
10      or technology used to encrypt and decrypt electronic  
11      messages and any product software or technology  
12      with encryption capabilities.

13          (8) KEY.—The term “key” means a parameter,  
14      or a component thereof, used with an algorithm to  
15      validate, authenticate, encrypt, or decrypt data or  
16      communications.

17          (9) KEY RECOVERY AGENT.—

18              (A) IN GENERAL.—The term “key recovery  
19      agent” means a person trusted by one or more  
20      persons to hold and maintain sufficient infor-  
21      mation to allow access to the data or commu-  
22      nications of the person or persons for whom  
23      that information is held, and who holds and  
24      maintains that information as a business or

1 governmental practice, whether or not for prof-  
2 it.

3 (B) INCLUSION.—The term “key recovery  
4 agent” includes any person who holds the per-  
5 son’s own recovery information.

6 (10) PERSON.—The term “person” means any  
7 individual, corporation, company, association, firm,  
8 partnership, society, or joint stock company.

9 (11) PLAINTEXT.—The term “plaintext” refers  
10 to data (including communications) that has not  
11 been encrypted or, if encrypted, has been decrypted.

12 (12) PUBLIC KEY.—The term “public key”  
13 means, for cryptographic systems that use different  
14 keys for encryption and decryption, the key that is  
15 intended to be publicly known.

16 (13) PUBLIC KEY CERTIFICATE.—The term  
17 “public key certificate” means information about a  
18 public key and its user, particularly including infor-  
19 mation that identifies that public key with its user,  
20 which has been digitally signed by the person issuing  
21 the public key certificate, using a private key of the  
22 issuer.

23 (14) QUALIFIED SYSTEM OF KEY RECOVERY.—  
24 The term “qualified system of key recovery” means  
25 a method of encryption which meets the criteria es-

1       tablished by the Secretary and provides for the re-  
2       covery of keys and may include the use of split keys,  
3       multiple key systems or other system approved by  
4       the Secretary, or a system which otherwise provides  
5       for the timely and unlawful access to plaintext, and  
6       meets the criteria established by the Secretary.

7           (15) RECOVERY INFORMATION.—The term “re-  
8       covery information” means a key or other informa-  
9       tion provided to a key recovery agent by a person  
10      that can be used to decrypt the data or communica-  
11      tions of the person.

12          (16) SECRETARY.—The term “Secretary”  
13      means the Secretary of Commerce.

14          (17) STATE.—The term “State” has the mean-  
15      ing given the term in section 2510(3) of title 18,  
16      United States Code.

17          (18) STORED ELECTRONIC INFORMATION.—The  
18      term “stored electronic information” means any wire  
19      communication or electronic communication that is  
20      in electronic storage.

21          (19) WIRE COMMUNICATION.—The term “wire  
22      communication” has the meaning given that term in  
23      section 2510(1) of title 18, United States Code.

○