

103^D CONGRESS
2^D SESSION

H. R. 5199

To amend the National Institute of Standards and Technology Act to provide for the establishment and management of voluntary encryption standards to protect the privacy and security of electronic information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 6, 1994

Mr. BROWN of California introduced the following bill; which was referred to the Committee on Science, Space, and Technology

A BILL

To amend the National Institute of Standards and Technology Act to provide for the establishment and management of voluntary encryption standards to protect the privacy and security of electronic information, and for other purposes.

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Encryption Standards
5 and Procedures Act of 1994”.

6 **SEC. 2. FINDINGS AND PURPOSES.**

7 (a) FINDINGS.—The Congress finds the following:

1 (1) Advancements in communications and infor-
2 mation technology and the widespread use of that
3 technology have enhanced the volume and value of
4 domestic and international communication of elec-
5 tronic information as well as the ability to preserve
6 the confidentiality, protect the privacy, and authen-
7 ticate the origin, of that information.

8 (2) The proliferation of communications and in-
9 formation technology has made it increasingly dif-
10 ficult for the government to obtain and decipher, in
11 a timely manner and as provided by law, electronic
12 information that is necessary to provide for public
13 safety and national security.

14 (3) The development of the Nation's informa-
15 tion infrastructure and the realization of the full
16 benefits of that infrastructure require that electronic
17 information resident in, or communicated over, that
18 infrastructure is secure, confidential, and authentic.

19 (4) Security, privacy, and authentication of
20 electronic information resident in, or communicated
21 over, the Nation's information infrastructure are en-
22 hanced with the use of encryption technology.

23 (5) The rights of individuals and other persons
24 to security, privacy, and protection in their commu-
25 nications and in the dissemination and receipt of

1 electronic information should be preserved and pro-
2 tected.

3 (6) The authority and ability of the government
4 to obtain and decipher, in a timely manner and as
5 provided by law, electronic information necessary to
6 provide for public safety and national security
7 should also be preserved.

8 (7) There is a national need to develop, adopt,
9 and use encryption methods and procedures that ad-
10 vance the development of the Nation's information
11 infrastructure and that preserve the personal rights
12 referred to in paragraph (5) and the governmental
13 authority and ability referred to in paragraph (6), as
14 provided by law.

15 (b) PURPOSES.—It is the purpose of this Act—

16 (1) to promote the development of the Nation's
17 information infrastructure consistent with public
18 welfare and safety, national security, and the privacy
19 and protection of personal property;

20 (2) to encourage and facilitate the development,
21 adoption, and use of encryption standards and pro-
22 cedures that provide sufficient privacy, protection,
23 and authentication of electronic information and
24 that reasonably satisfy the needs of government to
25 provide for public safety and national security; and

1 (3) to establish Federal policy governing the de-
2 velopment, adoption, and use of encryption stand-
3 ards and procedures and a Federal program to carry
4 out that policy.

5 **SEC. 3. ENCRYPTION STANDARDS AND PROCEDURES.**

6 (a) COMPUTER SYSTEM SECURITY AND PRIVACY AD-
7 VISORY BOARD.—

8 (1) REQUIREMENT OF PRIVACY EXPERTISE.—
9 Section 21(a)(2) of the National Institute of Stand-
10 ards and Technology Act (15 U.S.C. 278g-4(a)(2))
11 is amended by inserting “(including computer sys-
12 tems privacy)” after “related disciplines”.

13 (2) EXPANDED FUNCTIONS.—Section 21(b) of
14 such Act (15 U.S.C. 278g-4(b)) is amended—

15 (A) by striking “and” at the end of para-
16 graph (2);

17 (B) by striking the period at the end of
18 paragraph (3) and inserting “; and”; and

19 (C) by adding after paragraph (3) the fol-
20 lowing new paragraph:

21 “(4) to advise the Institute and the Congress
22 on privacy issues pertaining to electronic information
23 and on encryption standards developed under section
24 31(b).”.

1 (b) STANDARDS AND PROCEDURES.—The National
2 Institute of Standards and Technology Act is further
3 amended—

4 (1) by redesignating section 31 as section 32;
5 and

6 (2) by inserting after section 30 the following
7 new section 31:

8 **“SEC. 31. ENCRYPTION STANDARDS AND PROCEDURES.**

9 “(a) ESTABLISHMENT AND AUTHORITY.—The Sec-
10 retary, acting through the Director, shall establish an
11 Encryption Standards and Procedures Program to carry
12 out this section. In carrying out this section, the Sec-
13 retary, acting through the Director, may (in addition to
14 the authority provided under section 2) conduct research
15 and development on encryption standards and procedures,
16 make grants, and enter into contracts, cooperative agree-
17 ments, joint ventures, royalty arrangements, and licensing
18 agreements on such terms and conditions the Secretary
19 considers appropriate.

20 “(b) FEDERAL ENCRYPTION STANDARDS.—

21 “(1) IN GENERAL.—The Secretary, acting
22 through the Director and after providing notice to
23 the public and an opportunity for comment, may by
24 regulation develop encryption standards as part of
25 the program established under subsection (a).

1 “(2) REQUIREMENTS.—Any encryption stand-
2 ard developed under paragraph (1)—

3 “(A) shall, to the maximum extent prac-
4 ticable, provide for the confidentiality, integrity,
5 or authenticity of electronic information;

6 “(B) shall advance the development, and
7 enhance the security, of the Nation’s informa-
8 tion infrastructure;

9 “(C) shall contribute to public safety and
10 national security;

11 “(D) shall not diminish existing privacy
12 rights of individuals and other persons;

13 “(E) shall preserve the functional ability of
14 the government to decipher, in a timely man-
15 ner, electronic information that has been ob-
16 tained pursuant to an electronic surveillance
17 permitted by law;

18 “(F) may be implemented in software,
19 firmware, hardware, or any combination there-
20 of; and

21 “(G) shall include a validation program to
22 determine the extent to which such standards
23 have been implemented in conformance with the
24 requirements set forth in this paragraph.

1 “(3) CONSULTATION.—Standards developed
2 under paragraph (1) shall be developed in consulta-
3 tion with the heads of other appropriate Federal
4 agencies.

5 “(c) PERMITTED USE OF STANDARDS.—The Federal
6 Government shall make available for public use any stand-
7 ard established under subsection (b), except that nothing
8 in this Act may be construed to require such use by any
9 individual or other person.

10 “(d) ESCROW AGENTS.—

11 “(1) DESIGNATION.—If a key escrow encryption
12 standard is established under subsection (b), the
13 President shall designate at least 2 Federal agencies
14 that satisfy the qualifications referred to in para-
15 graph (2) to act as key escrow agents for that stand-
16 ard.

17 “(2) QUALIFICATIONS.—A key escrow agent
18 designated under paragraph (1) shall be a Federal
19 agency that—

20 “(A) possesses the capability, competency,
21 and resources to administer the key escrow
22 encryption standard, to safeguard sensitive in-
23 formation related to it, and to carry out the re-
24 sponsibilities set forth in paragraph (3) in a
25 timely manner; and

1 “(B) is not a Federal agency that is au-
2 thorized by law to conduct electronic surveil-
3 lance.

4 “(3) RESPONSIBILITIES.—A key escrow agent
5 designated under paragraph (1) shall, by regulation
6 and in consultation with the Secretary and any other
7 key escrow agent designated under such paragraph,
8 establish procedures and take other appropriate
9 steps—

10 “(A) to safeguard the confidentiality, in-
11 tegrity, and availability of keys or components
12 thereof held by the agent pursuant to this sub-
13 section;

14 “(B) to preserve the integrity of any key
15 escrow encryption standard established under
16 subsection (b) for which the agent holds the
17 keys or components thereof;

18 “(C) to hold and manage the keys or com-
19 ponents thereof consistent with the require-
20 ments of this section and the encryption stand-
21 ard established under subsection (b); and

22 “(D) to carry out the responsibilities set
23 forth in this paragraph in the most effective
24 and efficient manner practicable.

1 “(4) AUTHORITY.—A key escrow agent des-
2 ignated under paragraph (1) may enter into con-
3 tracts, cooperative agreements, and joint ventures
4 and take other appropriate steps to carry out its re-
5 sponsibilities.

6 “(e) LIMITATIONS ON ACCESS AND USE.—

7 “(1) RELEASE OF KEY TO CERTAIN AGEN-
8 CIES.—A key escrow agent designated under sub-
9 section (d) may release a key or component thereof
10 held by the agent pursuant to that subsection only
11 to a Federal agency that is authorized by law to con-
12 duct electronic surveillance and that is authorized to
13 obtain and use the key or component by court order
14 or other provision of law. An entity to whom a key
15 or component thereof has been released under this
16 paragraph may use the key or component thereof
17 only in the manner and for the purpose and dura-
18 tion that is expressly provided for in the court order
19 or other provision of law authorizing such release
20 and use.

21 “(2) LIMITATION ON USE BY PRIVATE PERSONS
22 AND FOREIGN CITIZENS.—

23 “(A) IN GENERAL.—Except as provided in
24 subparagraph (B), a person (including a person
25 not a citizen or permanent resident of the

1 United States) that is not an agency of the
2 Federal Government or a State or local govern-
3 ment shall not have access to or use keys asso-
4 ciated with an encryption standard established
5 under subsection (b).

6 “(B) EXCEPTION.—A representative of a
7 foreign government may have access to and use
8 a key associated with an encryption standard
9 established under subsection (b) only if the
10 President determines that such access and use
11 is in the national security and foreign policy in-
12 terests of the United States. The President
13 shall prescribe the manner and conditions of
14 any such access and use.

15 “(3) LIMIT ON USE BY GOVERNMENT AGEN-
16 CIES.—A government agency, instrumentality, or po-
17 litical subdivision thereof shall not have access to or
18 use a key or component thereof associated with an
19 encryption standard established under subsection (b)
20 that is held by a key escrow agent under subsection
21 (d) unless such access or use is authorized by this
22 section, by court order, or by other law.

23 “(f) REVIEW AND REPORT.—

24 “(1) IN GENERAL.—Within 2 years after the
25 date of the enactment of this Act and at least once

1 every 2 years thereafter, the Secretary shall conduct
2 a hearing on the record in which all interested par-
3 ties shall have an opportunity to comment on the ex-
4 tent to which encryption standards, procedures, and
5 requirements established under this section have
6 succeeded in fulfilling the purposes of this section
7 and the manner and extent to which such standards,
8 procedures, and requirements can be improved.

9 “(2) REPORT.—Upon completion of a hearing
10 conducted under paragraph (1), the Secretary shall
11 submit to the Congress a report containing a state-
12 ment of the Secretary’s findings pursuant to the
13 hearing along with recommendations and a plan for
14 correcting any deficiencies or abuses in achieving the
15 purposes of this section that are identified as a re-
16 sult of the hearing.

17 “(g) REGULATIONS.—Within one year after the date
18 of the enactment of this Act, the Secretary and each key
19 escrow agent designated by the President under subsection
20 (d) shall, after notice to the public and opportunity for
21 comment, issue any regulations necessary to carry out this
22 section.

23 “(h) LIABILITY.—The United States shall not be lia-
24 ble for any loss incurred by any individual or other person
25 resulting from any compromise or security breach of any

1 encryption standard established under subsection (b) or
2 any violation of this section or any regulation or procedure
3 established by or under this section by—

4 “(1) any person who is not an official or em-
5 ployee of the United States; or

6 “(2) any person who is an official or employee
7 of the United States, unless such compromise,
8 breach, or violation is willful.

9 “(i) SEVERABILITY.—If any provision of this section,
10 or the application thereof, to any person or circumstance,
11 is held invalid, the remainder of this section, and the ap-
12 plication thereof, to other persons or circumstances shall
13 not be affected thereby.

14 “(j) DEFINITIONS.—For purposes of this section:

15 “(1) The term ‘content’, when used with respect
16 to electronic information, includes the substance,
17 purport, or meaning of that information.

18 “(2) The term ‘electronic communications sys-
19 tem’ has the meaning given such term in section
20 2510(14) of title 18, United States Code.

21 “(3) The term ‘encryption’ means a method—

22 “(A) to encipher and decipher the content
23 of electronic information to protect the privacy
24 and security of such information; or

1 “(B) to verify the integrity, or authenticate
2 the origin, of electronic information.

3 “(4) The term ‘encryption standard’ means a
4 technical, management, physical, or administrative
5 standard or associated guideline or procedure for
6 conducting encryption, including key escrow
7 encryption, to ensure or verify the integrity, authen-
8 ticity, or confidentiality of electronic information
9 that, regardless of application or purpose, is stored,
10 processed, transmitted, or otherwise communicated
11 domestically or internationally in any public or pri-
12 vate electronic communications system.

13 “(5) The term ‘key escrow encryption’ means
14 an encryption method that allows the government,
15 pursuant to court order or other provision of law, to
16 decipher electronic information that has been
17 encrypted with that method by using a unique secret
18 code or key that is, in whole or in part, held by and
19 obtained from a key escrow agent.

20 “(6) The term ‘key escrow agent’ means an en-
21 tity designated by the President under subsection
22 (d) to hold and manage keys associated with an
23 encryption standard established under subsection
24 (b).

1 “(7) The term ‘key’ means a unique secret code
2 or character string that enables a party other than
3 the sender, holder, or intended recipient of electronic
4 information to decipher such information that has
5 been enciphered with a corresponding encryption
6 standard established under subsection (b) only with
7 such code or string.

8 “(8) The term ‘electronic information’ means
9 the content, source, or destination of any informa-
10 tion in any electronic form and in any medium which
11 has not been specifically authorized by a Federal
12 statute or an Executive Order to be kept secret in
13 the interest of national defense or foreign policy and
14 which is stored, processed, transmitted or otherwise
15 communicated, domestically or internationally, in an
16 electronic communications system, and

17 “(A) electronic communication within the
18 meaning of section 2510(12) of title 18, United
19 States Code; or

20 “(B) wire communication within the mean-
21 ing of section 2510(1) of such title.

22 “(9) The term ‘government’ means the Federal
23 Government, a State or political subdivision of a
24 State, the District of Columbia, or a commonwealth,
25 territory, or possession of the United States.

1 “(k) AUTHORIZATION OF APPROPRIATIONS.—

2 “(1) IN GENERAL.—From amounts otherwise
3 authorized to be appropriated to the Secretary of
4 Commerce for fiscal years 1995 through 1997 to
5 carry out the programs of the Institute, the amount
6 of \$50,000,000 shall be available for such fiscal
7 years to carry out this section. Such amount shall
8 remain available until expended. Of such amount,
9 \$1,000,000 shall be available for the National Re-
10 search Council study on national cryptography policy
11 authorized under section 267 of the National De-
12 fense Authorization Act for Fiscal Year 1994 (10
13 U.S.C 421 note).

14 “(2) TRANSFER AUTHORITY.—The Secretary
15 may transfer funds appropriated pursuant to para-
16 graph (1) to a key escrow agent other than the Sec-
17 retary in amounts sufficient to cover the cost of car-
18 rying out the responsibilities of the agent under this
19 section. Funds so transferred shall remain available
20 until expended.”.

○

HR 5199 IH—2