

106TH CONGRESS
1ST SESSION

H. R. 2413

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 1, 1999

Mr. SENSENBRENNER (for himself, Mr. GORDON, and Mrs. MORELLA)
introduced the following bill; which was referred to the Committee on Science

A BILL

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Computer Security
5 Enhancement Act of 1999”.

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

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

1 (1) The National Institute of Standards and
2 Technology has responsibility for developing stand-
3 ards and guidelines needed to ensure the cost-effec-
4 tive security and privacy of sensitive information in
5 Federal computer systems.

6 (2) The Federal Government has an important
7 role in ensuring the protection of sensitive, but un-
8 classified, information controlled by Federal agen-
9 cies.

10 (3) Technology that is based on the application
11 of cryptography exists and can be readily provided
12 by private sector companies to ensure the confiden-
13 tiality, authenticity, and integrity of information
14 associated with public and private activities.

15 (4) The development and use of encryption
16 technologies should be driven by market forces rath-
17 er than by Government imposed requirements.

18 (b) PURPOSES.—The purposes of this Act are to—

19 (1) reinforce the role of the National Institute
20 of Standards and Technology in ensuring the secu-
21 rity of unclassified information in Federal computer
22 systems; and

23 (2) promote technology solutions based on pri-
24 vate sector offerings to protect the security of Fed-
25 eral computer systems.

1 **SEC. 3. VOLUNTARY STANDARDS FOR PUBLIC KEY MAN-**
2 **AGEMENT INFRASTRUCTURE.**

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

5 (1) by redesignating paragraphs (2), (3), (4),
6 and (5) as paragraphs (3), (4), (7), and (8), respec-
7 tively; and

8 (2) by inserting after paragraph (1) the fol-
9 lowing new paragraph:

10 “(2) upon request from the private sector, to
11 assist in establishing voluntary interoperable stand-
12 ards, guidelines, and associated methods and tech-
13 niques to facilitate and expedite the establishment of
14 non-Federal management infrastructures for public
15 keys that can be used to communicate with and con-
16 duct transactions with the Federal Government;”.

17 **SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NET-**
18 **WORKS.**

19 Section 20(b) of the National Institute of Standards
20 and Technology Act (15 U.S.C. 278g–3(b)), as amended
21 by section 3 of this Act, is further amended by inserting
22 after paragraph (4), as so redesignated by section 3(1)
23 of this Act, the following new paragraphs:

24 “(5) to provide guidance and assistance to Fed-
25 eral agencies in the protection of interconnected
26 computer systems and to coordinate Federal re-

1 sponse efforts related to unauthorized access to Fed-
2 eral computer systems;

3 “(6) to perform evaluations and tests of—

4 “(A) information technologies to assess
5 security vulnerabilities; and

6 “(B) commercially available security prod-
7 ucts for their suitability for use by Federal
8 agencies for protecting sensitive information in
9 computer systems;”.

10 **SEC. 5. COMPUTER SECURITY IMPLEMENTATION.**

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

13 (1) by redesignating subsections (c) and (d) as
14 subsections (e) and (f), respectively; and

15 (2) by inserting after subsection (b) the fol-
16 lowing new subsection:

17 “(c) In carrying out subsection (a)(3), the Institute
18 shall—

19 “(1) emphasize the development of technology-
20 neutral policy guidelines for computer security prac-
21 tices by the Federal agencies;

22 “(2) actively promote the use of commercially
23 available products to provide for the security and
24 privacy of sensitive information in Federal computer
25 systems; and

1 “(3) participate in implementations of
2 encryption technologies in order to develop required
3 standards and guidelines for Federal computer sys-
4 tems, including assessing the desirability of and the
5 costs associated with establishing and managing key
6 recovery infrastructures for Federal Government in-
7 formation.”.

8 **SEC. 6. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS,**
9 **AND INFORMATION.**

10 Section 20 of the National Institute of Standards and
11 Technology Act (15 U.S.C. 278g-3), as amended by this
12 Act, is further amended by inserting after subsection (c),
13 as added by section 5 of this Act, the following new sub-
14 section:

15 “(d)(1) The Institute shall solicit the recommenda-
16 tions of the Computer System Security and Privacy Advi-
17 sory Board, established by section 21, regarding standards
18 and guidelines that are being considered for submittal to
19 the Secretary in accordance with subsection (a)(4). No
20 standards or guidelines shall be submitted to the Secretary
21 prior to the receipt by the Institute of the Board’s written
22 recommendations. The recommendations of the Board
23 shall accompany standards and guidelines submitted to
24 the Secretary.

1 “(2) There are authorized to be appropriated to the
2 Secretary \$1,000,000 for fiscal year 2000 and \$1,030,000
3 for fiscal year 2001 to enable the Computer System Secu-
4 rity and Privacy Advisory Board, established by section
5 21, to identify emerging issues related to computer secu-
6 rity, privacy, and cryptography and to convene public
7 meetings on those subjects, receive presentations, and
8 publish reports, digests, and summaries for public dis-
9 tribution on those subjects.”.

10 **SEC. 7. LIMITATION ON PARTICIPATION IN REQUIRING**
11 **ENCRYPTION STANDARDS.**

12 Section 20 of the National Institute of Standards and
13 Technology Act (15 U.S.C. 278g-3), as amended by this
14 Act, is further amended by adding at the end the following
15 new subsection:

16 “(g) The Institute shall not promulgate, enforce, or
17 otherwise adopt standards, or carry out activities or poli-
18 cies, for the Federal establishment of encryption standards
19 required for use in computer systems other than Federal
20 Government computer systems.”.

21 **SEC. 8. MISCELLANEOUS AMENDMENTS.**

22 Section 20 of the National Institute of Standards and
23 Technology Act (15 U.S.C. 278g-3), as amended by this
24 Act, is further amended—

1 (1) in subsection (b)(8), as so redesignated by
2 section 3(1) of this Act, by inserting “to the extent
3 that such coordination will improve computer secu-
4 rity and to the extent necessary for improving such
5 security for Federal computer systems” after “Man-
6 agement and Budget”;

7 (2) in subsection (e), as so redesignated by sec-
8 tion 5(1) of this Act, by striking “shall draw upon”
9 and inserting in lieu thereof “may draw upon”;

10 (3) in subsection (e)(2), as so redesignated by
11 section 5(1) of this Act, by striking “(b)(5)” and in-
12 serting in lieu thereof “(b)(8)”; and

13 (4) in subsection (f)(1)(B)(i), as so redesign-
14 ated by section 5(1) of this Act, by inserting “and
15 computer networks” after “computers”.

16 **SEC. 9. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.**

17 Section 5(b) of the Computer Security Act of 1987
18 (49 U.S.C. 759 note) is amended—

19 (1) by striking “and” at the end of paragraph
20 (1);

21 (2) by striking the period at the end of para-
22 graph (2) and inserting in lieu thereof “; and”; and

23 (3) by adding at the end the following new
24 paragraph:

1 (b) CONTENTS.—The study referred to in subsection

2 (a) shall—

3 (1) assess technology needed to support public
4 key infrastructures;

5 (2) assess current public and private plans for
6 the deployment of public key infrastructures;

7 (3) assess interoperability, scalability, and in-
8 tegrity of private and public entities that are ele-
9 ments of public key infrastructures;

10 (4) make recommendations for Federal legisla-
11 tion and other Federal actions required to ensure
12 the national feasibility and utility of public key in-
13 frastructures; and

14 (5) address such other matters as the National
15 Research Council considers relevant to the issues of
16 public key infrastructure.

17 (c) INTERAGENCY COOPERATION WITH STUDY.—All
18 agencies of the Federal Government shall cooperate fully
19 with the National Research Council in its activities in car-
20 rying out the study under this section, including access
21 by properly cleared individuals to classified information if
22 necessary.

23 (d) REPORT.—Not later than 18 months after the
24 date of the enactment of this Act, the Secretary of Com-
25 merce shall transmit to the Committee on Science of the

1 House of Representatives and the Committee on Com-
2 merce, Science, and Transportation of the Senate a report
3 setting forth the findings, conclusions, and recommenda-
4 tions of the National Research Council for public policy
5 related to public key infrastructures for use by individuals,
6 businesses, and government. Such report shall be sub-
7 mitted in unclassified form.

8 (e) AUTHORIZATION OF APPROPRIATIONS.—There
9 are authorized to be appropriated to the Secretary of Com-
10 merce \$450,000 for fiscal year 2000, to remain available
11 until expended, for carrying out this section.

12 **SEC. 12. PROMOTION OF NATIONAL INFORMATION SECU-**
13 **RITY.**

14 The Under Secretary of Commerce for Technology
15 shall—

16 (1) promote the more widespread use of appli-
17 cations of cryptography and associated technologies
18 to enhance the security of the Nation's information
19 infrastructure;

20 (2) establish a central clearinghouse for the col-
21 lection by the Federal Government and dissemina-
22 tion to the public of information to promote aware-
23 ness of information security threats; and

24 (3) promote the development of the national,
25 standards-based infrastructure needed to support

1 commercial and private uses of encryption tech-
2 nologies for confidentiality and authentication.

3 **SEC. 13. ELECTRONIC AUTHENTICATION INFRASTRUC-**
4 **TURE.**

5 (a) ELECTRONIC AUTHENTICATION INFRASTRUC-
6 TURE.—

7 (1) GUIDELINES AND STANDARDS.—Not later
8 than 1 year after the date of the enactment of this
9 Act, the Director, in consultation with industry,
10 shall develop electronic authentication infrastructure
11 guidelines and standards for use by Federal agencies
12 to enable those agencies to effectively utilize elec-
13 tronic authentication technologies in a manner that
14 is—

15 (A) sufficiently secure to meet the needs of
16 those agencies and their transaction partners;
17 and

18 (B) interoperable, to the maximum extent
19 possible.

20 (2) ELEMENTS.—The guidelines and standards
21 developed under paragraph (1) shall include—

22 (A) protection profiles for cryptographic
23 and noncryptographic methods of authen-
24 ticating identity for electronic authentication
25 products and services;

1 (B) minimum interoperability specifica-
2 tions for the Federal acquisition of electronic
3 authentication products and services; and

4 (C) validation criteria to enable Federal
5 agencies to select cryptographic electronic au-
6 thentication products and services appropriate
7 to their needs.

8 (3) COORDINATION WITH NATIONAL POLICY
9 PANEL.—The Director shall ensure that the develop-
10 ment of guidelines and standards with respect to
11 cryptographic electronic authentication products and
12 services under this subsection is carried out in co-
13 ordination with the efforts of the National Policy
14 Panel for Digital Signatures under subsection (e).

15 (4) REVISIONS.—The Director shall periodically
16 review the guidelines and standards developed under
17 paragraph (1) and revise them as appropriate.

18 (b) VALIDATION OF PRODUCTS.—Not later than 1
19 year after the date of the enactment of this Act, and there-
20 after, the Director shall maintain and make available to
21 Federal agencies and to the public a list of commercially
22 available electronic authentication products, and other
23 such products used by Federal agencies, evaluated as con-
24 forming with the guidelines and standards developed
25 under subsection (a).

1 (c) ELECTRONIC CERTIFICATION AND MANAGEMENT
2 SYSTEMS.—

3 (1) CRITERIA.—Not later than 1 year after the
4 date of the enactment of this Act, the Director shall
5 establish minimum technical criteria for the use by
6 Federal agencies of electronic certification and man-
7 agement systems.

8 (2) EVALUATION.—The Director shall establish
9 a program for evaluating the conformance with the
10 criteria established under paragraph (1) of electronic
11 certification and management systems, developed for
12 use by Federal agencies or available for such use.

13 (3) MAINTENANCE OF LIST.—The Director
14 shall maintain and make available to Federal agen-
15 cies a list of electronic certification and management
16 systems evaluated as conforming to the criteria es-
17 tablished under paragraph (1).

18 (d) REPORTS.—Not later than 18 months after the
19 date of the enactment of this Act, and annually thereafter,
20 the Director shall transmit to the Congress a report that
21 includes—

22 (1) a description and analysis of the utilization
23 by Federal agencies of electronic authentication
24 technologies;

1 (2) an evaluation of the extent to which Federal
2 agencies' electronic authentication infrastructures
3 conform to the guidelines and standards developed
4 under subsection (a)(1);

5 (3) an evaluation of the extent to which Federal
6 agencies' electronic certification and management
7 systems conform to the criteria established under
8 subsection (c)(1);

9 (4) the list described in subsection (c)(3); and

10 (5) evaluations made under subsection (b).

11 (e) NATIONAL POLICY PANEL FOR DIGITAL SIGNA-
12 TURES.—

13 (1) ESTABLISHMENT.—Not later than 90 days
14 after the date of the enactment of this Act, the
15 Under Secretary shall establish a National Policy
16 Panel for Digital Signatures. The Panel shall be
17 composed of government, academic, and industry
18 technical and legal experts on the implementation of
19 digital signature technologies, State officials, includ-
20 ing officials from States which have enacted laws
21 recognizing the use of digital signatures, and rep-
22 resentative individuals from the interested public.

23 (2) RESPONSIBILITIES.—The Panel shall serve
24 as a forum for exploring all relevant factors associ-
25 ated with the development of a national digital sig-

1 nature infrastructure based on uniform guidelines
2 and standards to enable the widespread availability
3 and use of digital signature systems. The Panel shall
4 develop—

5 (A) model practices and procedures for
6 certification authorities to ensure the accuracy,
7 reliability, and security of operations associated
8 with issuing and managing digital certificates;

9 (B) guidelines and standards to ensure
10 consistency among jurisdictions that license cer-
11 tification authorities; and

12 (C) audit procedures for certification au-
13 thorities.

14 (3) COORDINATION.—The Panel shall coordi-
15 nate its efforts with those of the Director under sub-
16 section (a).

17 (4) ADMINISTRATIVE SUPPORT.—The Under
18 Secretary shall provide administrative support to en-
19 able the Panel to carry out its responsibilities.

20 (5) REPORT.—Not later than 1 year after the
21 date of the enactment of this Act, the Under Sec-
22 retary shall transmit to the Congress a report con-
23 taining the recommendations of the Panel.

24 (f) DEFINITIONS.—For purposes of this section—

1 (1) the term “certification authorities” means
2 issuers of digital certificates;

3 (2) the term “digital certificate” means an elec-
4 tronic document that binds an individual’s identity
5 to the individual’s key;

6 (3) the term “digital signature” means a math-
7 ematically generated mark utilizing key cryptog-
8 raphy techniques that is unique to both the signa-
9 tory and the information signed;

10 (4) the term “digital signature infrastructure”
11 means the software, hardware, and personnel re-
12 sources, and the procedures, required to effectively
13 utilize digital certificates and digital signatures;

14 (5) the term “electronic authentication” means
15 cryptographic or noncryptographic methods of au-
16 thenticating identity in an electronic communication;

17 (6) the term “electronic authentication infra-
18 structure” means the software, hardware, and per-
19 sonnel resources, and the procedures, required to ef-
20 fectively utilize electronic authentication tech-
21 nologies;

22 (7) the term “electronic certification and man-
23 agement systems” means computer systems, includ-
24 ing associated personnel and procedures, that enable

1 individuals to apply unique digital signatures to elec-
2 tronic information;

3 (8) the term “protection profile” means a list of
4 security functions and associated assurance levels
5 used to describe a product; and

6 (9) the term “Under Secretary” means the
7 Under Secretary of Commerce for Technology.

8 **SEC. 14. SOURCE OF AUTHORIZATIONS.**

9 There are authorized to be appropriated to the Sec-
10 retary of Commerce \$3,000,000 for fiscal year 2000 and
11 \$4,000,000 for fiscal year 2001, for the National Institute
12 of Standards and Technology to carry out activities au-
13 thorized by this Act for which funds are not otherwise spe-
14 cifically authorized to be appropriated by this Act.

○