

Union Calendar No. 527

106TH CONGRESS
2^D SESSION

H. R. 2413

[Report No. 106-876]

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

SEPTEMBER 21, 2000

Additional sponsors: Mr. EHLERS, Mr. COOK, Mr. EWING, Mr. GUTKNECHT, and Mr. KUYKENDALL

SEPTEMBER 21, 2000

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italic*]

[For text of introduced bill, see copy of bill as introduced on July 21, 1999]

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 2000”.*

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

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

8 *(1) The National Institute of Standards and*
9 *Technology has responsibility for developing stand-*
10 *ards and guidelines needed to ensure the cost-effective*
11 *security and privacy of sensitive information in Fed-*
12 *eral computer systems.*

13 *(2) The Federal Government has an important*
14 *role in ensuring the protection of sensitive, but un-*
15 *classified, information controlled by Federal agencies.*

16 *(3) Technology that is based on the application*
17 *of cryptography exists and can be readily provided by*
18 *private sector companies to ensure the confidentiality,*
19 *authenticity, and integrity of information associated*
20 *with public and private activities.*

21 *(4) The development and use of encryption tech-*
22 *nologies by industry should be driven by market*
23 *forces rather than by Government imposed require-*
24 *ments.*

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

1 (1) reinforce the role of the National Institute of
2 Standards and Technology in ensuring the security of
3 unclassified information in Federal computer systems;
4 and

5 (2) promote technology solutions based on pri-
6 vate sector offerings to protect the security of Federal
7 computer systems.

8 **SEC. 3. VOLUNTARY STANDARDS FOR PUBLIC KEY MANAGE-**
9 **MENT INFRASTRUCTURE.**

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

12 (1) by redesignating paragraphs (2), (3), (4),
13 and (5) as paragraphs (3), (4), (8), and (9), respec-
14 tively; and

15 (2) by inserting after paragraph (1) the fol-
16 lowing new paragraph:

17 “(2) upon request from the private sector, to as-
18 sist in establishing voluntary interoperable standards,
19 guidelines, and associated methods and techniques to
20 facilitate and expedite the establishment of non-Fed-
21 eral management infrastructures for public keys that
22 can be used to communicate with and conduct trans-
23 actions with the Federal Government;”.

1 **SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NET-**
2 **WORKS.**

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

8 *“(5) except for national security systems, as de-*
9 *finied in section 5142 of Public Law 104-106 (40*
10 *U.S.C. 1452), to provide guidance and assistance to*
11 *Federal agencies for protecting the security and pri-*
12 *vacv of sensitive information in interconnected Fed-*
13 *eral computer systems, including identification of sig-*
14 *nificant risks thereto;*

15 *“(6) to promote compliance by Federal agencies*
16 *with existing Federal computer information security*
17 *and privacy guidelines;*

18 *“(7) in consultation with appropriate Federal*
19 *agencies, assist Federal response efforts related to un-*
20 *authorized access to Federal computer systems;”.*

21 **SEC. 5. COMPUTER SECURITY IMPLEMENTATION.**

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

24 *(1) by redesignating subsections (c) and (d) as*
25 *subsections (e) and (f), respectively; and*

1 (2) by inserting after subsection (b) the following
2 new subsection:

3 “(c)(1) In carrying out subsection (a)(2) and (3), the
4 Institute shall—

5 “(A) emphasize the development of technology-
6 neutral policy guidelines for computer security prac-
7 tices by the Federal agencies;

8 “(B) promote the use of commercially available
9 products, which appear on the list required by para-
10 graph (2), to provide for the security and privacy of
11 sensitive information in Federal computer systems;

12 “(C) develop qualitative and quantitative meas-
13 ures appropriate for assessing the quality and effec-
14 tiveness of information security and privacy pro-
15 grams at Federal agencies;

16 “(D) perform evaluations and tests at Federal
17 agencies to assess existing information security and
18 privacy programs;

19 “(E) promote development of accreditation proce-
20 dures for Federal agencies based on the measures de-
21 veloped under subparagraph (C);

22 “(F) if requested, consult with and provide as-
23 sistance to Federal agencies regarding the selection by
24 agencies of security technologies and products and the
25 implementation of security practices; and

1 “(G)(i) develop uniform testing procedures suit-
2 able for determining the conformance of commercially
3 available security products to the guidelines and
4 standards developed under subsection (a)(2) and (3);

5 “(ii) establish procedures for certification of pri-
6 vate sector laboratories to perform the tests and eval-
7 uations of commercially available security products
8 developed in accordance with clause (i); and

9 “(iii) promote the testing of commercially avail-
10 able security products for their conformance with
11 guidelines and standards developed under subsection
12 (a)(2) and (3).

13 “(2) The Institute shall maintain and make available
14 to Federal agencies and to the public a list of commercially
15 available security products that have been tested by private
16 sector laboratories certified in accordance with procedures
17 established under paragraph (1)(G)(ii), and that have been
18 found to be in conformance with the guidelines and stand-
19 ards developed under subsection (a)(2) and (3).

20 “(3) The Institute shall annually transmit to the Con-
21 gress, in an unclassified format, a report containing—

22 “(A) the findings of the evaluations and tests of
23 Federal computer systems conducted under this sec-
24 tion during the 12 months preceding the date of the
25 report, including the frequency of the use of commer-

1 *cially available security products included on the list*
2 *required by paragraph (2);*

3 *“(B) the planned evaluations and tests under*
4 *this section for the 12 months following the date of the*
5 *report; and*

6 *“(C) any recommendations by the Institute to*
7 *Federal agencies resulting from the findings described*
8 *in subparagraph (A), and the response by the agen-*
9 *cies to those recommendations.”.*

10 **SEC. 6. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS,**
11 **AND INFORMATION.**

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

16 *“(d)(1) The Institute shall solicit the recommendations*
17 *of the Computer System Security and Privacy Advisory*
18 *Board, established by section 21, regarding standards and*
19 *guidelines that are being considered for submittal to the*
20 *Secretary in accordance with subsection (a)(4). The rec-*
21 *ommendations of the Board shall accompany standards and*
22 *guidelines submitted to the Secretary.*

23 *“(2) There are authorized to be appropriated to the*
24 *Secretary \$1,030,000 for fiscal year 2001 and \$1,060,000*
25 *for fiscal year 2002 to enable the Computer System Security*

1 *and Privacy Advisory Board, established by section 21, to*
2 *identify emerging issues related to computer security, pri-*
3 *vacy, and cryptography and to convene public meetings on*
4 *those subjects, receive presentations, and publish reports, di-*
5 *gests, and summaries for public distribution on those sub-*
6 *jects.”.*

7 **SEC. 7. LIMITATION ON PARTICIPATION IN REQUIRING**
8 **ENCRYPTION STANDARDS.**

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

13 *“(g) The Institute shall not promulgate, enforce, or oth-*
14 *erwise adopt standards, or carry out activities or policies,*
15 *for the Federal establishment of encryption standards re-*
16 *quired for use in computer systems other than Federal Gov-*
17 *ernment computer systems.”.*

18 **SEC. 8. MISCELLANEOUS AMENDMENTS.**

19 *Section 20 of the National Institute of Standards and*
20 *Technology Act (15 U.S.C. 278g–3), as amended by this Act,*
21 *is further amended—*

22 *(1) in subsection (b)(9), as so redesignated by*
23 *section 3(1) of this Act, by inserting “to the extent*
24 *that such coordination will improve computer secu-*
25 *rity and to the extent necessary for improving such*

1 *security for Federal computer systems” after “Man-*
2 *agement and Budget)”;*

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

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

9 *(4) in subsection (f)(1)(B)(i), as so redesignated*
10 *by section 5(1) of this Act, by inserting “and com-*
11 *puter networks” after “computers”.*

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

13 *Section 5(b) of the Computer Security Act of 1987 (40*
14 *U.S.C. 759 note) is amended—*

15 *(1) by striking “and” at the end of paragraph*
16 *(1);*

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

19 *(3) by adding at the end the following new para-*
20 *graph:*

21 *“(3) to include emphasis on protecting sensitive*
22 *information in Federal databases and Federal com-*
23 *puter sites that are accessible through public net-*
24 *works.”.*

1 **SEC. 10. COMPUTER SECURITY FELLOWSHIP PROGRAM.**

2 *There are authorized to be appropriated to the Sec-*
3 *retary of Commerce \$500,000 for fiscal year 2001 and*
4 *\$500,000 for fiscal year 2002 for the Director of the Na-*
5 *tional Institute of Standards and Technology for fellow-*
6 *ships, subject to the provisions of section 18 of the National*
7 *Institute of Standards and Technology Act (15 U.S.C.*
8 *278g–1), to support students at institutions of higher learn-*
9 *ing in computer security. Amounts authorized by this sec-*
10 *tion shall not be subject to the percentage limitation stated*
11 *in such section 18.*

12 **SEC. 11. STUDY OF PUBLIC KEY INFRASTRUCTURE BY THE**
13 **NATIONAL RESEARCH COUNCIL.**

14 *(a) REVIEW BY NATIONAL RESEARCH COUNCIL.—Not*
15 *later than 90 days after the date of the enactment of this*
16 *Act, the Secretary of Commerce shall enter into a contract*
17 *with the National Research Council of the National Acad-*
18 *emy of Sciences to conduct a study of public key infrastruc-*
19 *tures for use by individuals, businesses, and government.*

20 *(b) CONTENTS.—The study referred to in subsection*
21 *(a) shall—*

22 *(1) assess technology needed to support public*
23 *key infrastructures;*

24 *(2) assess current public and private plans for*
25 *the deployment of public key infrastructures;*

1 (3) *assess interoperability, scalability, and integ-*
2 *riety of private and public entities that are elements*
3 *of public key infrastructures;*

4 (4) *make recommendations for Federal legisla-*
5 *tion and other Federal actions required to ensure the*
6 *national feasibility and utility of public key infra-*
7 *structures; and*

8 (5) *address such other matters as the National*
9 *Research Council considers relevant to the issues of*
10 *public key infrastructure.*

11 (c) *INTERAGENCY COOPERATION WITH STUDY.—All*
12 *agencies of the Federal Government shall cooperate fully*
13 *with the National Research Council in its activities in car-*
14 *rying out the study under this section, including access by*
15 *properly cleared individuals to classified information if*
16 *necessary.*

17 (d) *REPORT.—Not later than 18 months after the date*
18 *of the enactment of this Act, the Secretary of Commerce*
19 *shall transmit to the Committee on Science of the House*
20 *of Representatives and the Committee on Commerce,*
21 *Science, and Transportation of the Senate a report setting*
22 *forth the findings, conclusions, and recommendations of the*
23 *National Research Council for public policy related to pub-*
24 *lic key infrastructures for use by individuals, businesses,*

1 *and government. Such report shall be submitted in unclassi-*
2 *fied form.*

3 *(e) AUTHORIZATION OF APPROPRIATIONS.—There are*
4 *authorized to be appropriated to the Secretary of Commerce*
5 *\$450,000 for fiscal year 2001, to remain available until ex-*
6 *pended, for carrying out this section.*

7 **SEC. 12. PROMOTION OF NATIONAL INFORMATION SECUR-**
8 **RITY.**

9 *The Under Secretary of Commerce for Technology*
10 *shall—*

11 *(1) promote an increased use of security tech-*
12 *niques, such as risk assessment, and security tools,*
13 *such as cryptography, to enhance the protection of the*
14 *Nation’s information infrastructure;*

15 *(2) establish a central repository of information*
16 *for dissemination to the public to promote awareness*
17 *of information security vulnerabilities and risks; and*

18 *(3) promote the development of the national,*
19 *standards-based infrastructure needed to support gov-*
20 *ernment, commercial, and private uses of encryption*
21 *technologies for confidentiality and authentication.*

22 **SEC. 13. ELECTRONIC AUTHENTICATION INFRASTRUCTURE.**

23 *(a) ELECTRONIC AUTHENTICATION INFRASTRUC-*
24 *TURE.—*

1 (1) *GUIDELINES AND STANDARDS.*—Not later
2 than 18 months after the date of the enactment of this
3 Act, the Director, in consultation with industry and
4 appropriate Federal agencies, shall develop electronic
5 authentication infrastructure guidelines and stand-
6 ards for use by Federal agencies to assist those agen-
7 cies to effectively select and utilize electronic authen-
8 tication technologies in a manner that is—

9 (A) *adequately secure to meet the needs of*
10 *those agencies and their transaction partners;*
11 *and*

12 (B) *interoperable, to the maximum extent*
13 *possible.*

14 (2) *ELEMENTS.*—The guidelines and standards
15 developed under paragraph (1) shall include—

16 (A) *protection profiles for cryptographic*
17 *and noncryptographic methods of authenticating*
18 *identity for electronic authentication products*
19 *and services;*

20 (B) *a core set of interoperability specifica-*
21 *tions for the Federal acquisition of electronic au-*
22 *thentication products and services; and*

23 (C) *validation criteria to enable Federal*
24 *agencies to select cryptographic electronic au-*

1 *thentication products and services appropriate to*
2 *their needs.*

3 (3) *COORDINATION WITH NATIONAL POLICY*
4 *PANEL.—The Director shall ensure that the develop-*
5 *ment of guidelines and standards with respect to*
6 *cryptographic electronic authentication products and*
7 *services under this subsection is carried out in con-*
8 *sultation with the National Policy Panel for Digital*
9 *Signatures established under subsection (e).*

10 (4) *REVISIONS.—The Director shall periodically*
11 *review the guidelines and standards developed under*
12 *paragraph (1) and revise them as appropriate.*

13 (b) *LISTING OF VALIDATED PRODUCTS.—Not later*
14 *than 30 months after the date of the enactment of this Act,*
15 *and thereafter, the Director shall maintain and make avail-*
16 *able to Federal agencies and to the public a list of commer-*
17 *cially available electronic authentication products, and*
18 *other such products used by Federal agencies, evaluated as*
19 *conforming with the guidelines and standards developed*
20 *under subsection (a).*

21 (c) *SPECIFICATIONS FOR ELECTRONIC CERTIFICATION*
22 *AND MANAGEMENT TECHNOLOGIES.—*

23 (1) *SPECIFICATIONS.—The Director shall, as ap-*
24 *propriate, establish core specifications for particular*

1 *electronic certification and management technologies,*
2 *or their components, for use by Federal agencies.*

3 (2) *EVALUATION.*—*The Director shall advise*
4 *Federal agencies on how to evaluate the conformance*
5 *with the specifications established under paragraph*
6 *(1) of electronic certification and management tech-*
7 *nologies, developed for use by Federal agencies or*
8 *available for such use.*

9 (3) *MAINTENANCE OF LIST.*—*The Director shall*
10 *maintain and make available to Federal agencies a*
11 *list of electronic certification and management tech-*
12 *nologies evaluated as conforming to the specifications*
13 *established under paragraph (1).*

14 (d) *REPORTS.*—*Not later than 18 months after the*
15 *date of the enactment of this Act, and annually thereafter,*
16 *the Director shall transmit to the Congress a report that*
17 *includes—*

18 (1) *a description and analysis of the utilization*
19 *by Federal agencies of electronic authentication tech-*
20 *nologies; and*

21 (2) *an evaluation of the extent to which Federal*
22 *agencies' electronic authentication infrastructures*
23 *conform to the guidelines and standards developed*
24 *under subsection (a)(1).*

1 (e) *NATIONAL POLICY PANEL FOR DIGITAL SIGNA-*
2 *TURES.—*

3 (1) *ESTABLISHMENT.—Not later than 90 days*
4 *after the date of the enactment of this Act, the Under*
5 *Secretary shall establish a National Policy Panel for*
6 *Digital Signatures. The Panel shall be composed of*
7 *government, academic, and industry technical and*
8 *legal experts on the implementation of digital signa-*
9 *ture technologies, State officials, including officials*
10 *from States which have enacted laws recognizing the*
11 *use of digital signatures, and representative individ-*
12 *uals from the interested public.*

13 (2) *RESPONSIBILITIES.—The Panel shall serve as*
14 *a forum for exploring all relevant factors associated*
15 *with the development of a national digital signature*
16 *infrastructure based on uniform guidelines and stand-*
17 *ards to enable the widespread availability and use of*
18 *digital signature systems. The Panel shall develop—*

19 (A) *model practices and procedures for cer-*
20 *tification authorities to ensure the accuracy, reli-*
21 *ability, and security of operations associated*
22 *with issuing and managing digital certificates;*

23 (B) *guidelines and standards to ensure con-*
24 *sistency among jurisdictions that license certifi-*
25 *cation authorities; and*

1 (C) *audit procedures for certification au-*
2 *thorities.*

3 (3) *COORDINATION.*—*The Panel shall coordinate*
4 *its efforts with those of the Director under subsection*
5 *(a).*

6 (4) *ADMINISTRATIVE SUPPORT.*—*The Under Sec-*
7 *retary shall provide administrative support to enable*
8 *the Panel to carry out its responsibilities.*

9 (5) *REPORT.*—*Not later than 1 year after the*
10 *date of the enactment of this Act, the Under Secretary*
11 *shall transmit to the Congress a report containing the*
12 *recommendations of the Panel.*

13 (f) *DEFINITIONS.*—*For purposes of this section—*

14 (1) *the term “certification authorities” means*
15 *issuers of digital certificates;*

16 (2) *the term “digital certificate” means an elec-*
17 *tronic document that binds an individual’s identity*
18 *to the individual’s key;*

19 (3) *the term “digital signature” means a mathe-*
20 *matically generated mark utilizing key cryptography*
21 *techniques that is unique to both the signatory and*
22 *the information signed;*

23 (4) *the term “digital signature infrastructure”*
24 *means the software, hardware, and personnel re-*

1 sources, and the procedures, required to effectively uti-
2 lize digital certificates and digital signatures;

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

6 (6) the term “electronic authentication infra-
7 structure” means the software, hardware, and per-
8 sonnel resources, and the procedures, required to effec-
9 tively utilize electronic authentication technologies;

10 (7) the term “electronic certification and man-
11 agement technologies” means computer systems, in-
12 cluding associated personnel and procedures, that en-
13 able individuals to apply unique digital signatures to
14 electronic information;

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

18 (9) the term “Under Secretary” means the
19 Under Secretary of Commerce for Technology.

20 **SEC. 14. SOURCE OF AUTHORIZATIONS.**

21 There are authorized to be appropriated to the Sec-
22 retary of Commerce \$7,000,000 for fiscal year 2001 and
23 \$8,000,000 for fiscal year 2002, for the National Institute
24 of Standards and Technology to carry out activities author-

1 *ized by this Act for which funds are not otherwise specifi-*
2 *cally authorized to be appropriated by this Act.*

Union Calendar No. 527

106TH CONGRESS
2D SESSION

H. R. 2413

[Report No. 106-876]

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.

SEPTEMBER 21, 2000

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed