

107TH CONGRESS
2D SESSION

S. 1900

To protect against cyberterrorism and cybercrime, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JANUARY 28, 2002

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

A BILL

To protect against cyberterrorism and cybercrime, 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 “Cyberterrorism Pre-
5 paredness Act of 2002”.

6 **SEC. 2. GRANT FOR PROGRAM FOR PROTECTION OF INFOR-**
7 **MATION INFRASTRUCTURE AGAINST DISRUP-**
8 **TION.**

9 (a) IN GENERAL.—The National Institute of Stand-
10 ards and Technology shall, using amounts authorized to
11 be appropriated by section 5, award a grant to a qualifying

1 nongovernmental entity for purposes of a program to sup-
2 port the development of appropriate cybersecurity best
3 practices, support long-term cybersecurity research and
4 development, and perform functions relating to such ac-
5 tivities. The purpose of the program shall be to provide
6 protection for the information infrastructure of the United
7 States against terrorist or other disruption or attack or
8 other unwarranted intrusion.

9 (b) QUALIFYING NONGOVERNMENTAL ENTITY.—For
10 purposes of this section, a qualifying nongovernmental en-
11 tity is any entity that—

12 (1) is a nonprofit, nongovernmental consortium
13 composed of at least three academic centers of ex-
14 pertise in cybersecurity and at least three private
15 sector centers of expertise in cybersecurity;

16 (2) has a board of directors of at least 12 mem-
17 bers who include senior administrators of academic
18 centers of expertise in cybersecurity and senior man-
19 agers of private sector centers of expertise in
20 cybersecurity and of whom not more than one third
21 are affiliated with the centers comprising the consor-
22 tium;

23 (3) is operated by individuals from academia,
24 the private sector, or both who have—

1 (A) a demonstrated expertise in
2 cybersecurity; and

3 (B) the capacity to carry out the program
4 required under subsection (g);

5 (4) has in place a set of rules to ensure that
6 conflicts of interest involving officers, employees,
7 and members of the board of directors of the entity
8 do not undermine the activities of the entity;

9 (5) has developed a detailed plan for the pro-
10 gram required under subsection (g); and

11 (6) meets any other requirements established by
12 the National Institute of Standards and Technology
13 for purposes of this Act.

14 (c) APPLICATION.—Any entity seeking a grant under
15 this section shall submit to the National Institute of
16 Standards and Technology an application therefor, in such
17 form and containing such information as the National In-
18 stitute for Standards and Technology shall require.

19 (d) SELECTION OF GRANTEE.—The entity awarded
20 a grant under this section shall be selected after full and
21 open competition among qualifying nongovernmental enti-
22 ties.

23 (e) DISPERSAL OF GRANT AMOUNT.—Amounts avail-
24 able for the grant under this section pursuant to the au-
25 thorization of appropriations in section 5 shall be dis-

1 persed on a fiscal year basis over the five fiscal years be-
2 ginning with fiscal year 2003.

3 (f) CONSULTATION.—In carrying out activities under
4 this section, including selecting an entity for the award
5 of a grant, dispersing grant amounts, and overseeing ac-
6 tivities of the entity receiving the grant, the National In-
7 stitute of Standards and Technology—

8 (1) shall consult with an existing interagency
9 entity, or new interagency entity, consisting of the
10 elements of the Federal Government having a sub-
11 stantial interest and expertise in cybersecurity and
12 designated by the President for purposes of this Act;
13 and

14 (2) may consult separately with any such ele-
15 ment of the Federal Government.

16 (g) PROGRAM USING GRANT AMOUNT.—

17 (1) IN GENERAL.—The entity awarded a grant
18 under this section shall carry out a national program
19 for the purpose of protecting the information infra-
20 structure of the United States against disruption.
21 The program shall consist of—

22 (A) multi-disciplinary research and devel-
23 opment to identify appropriate cybersecurity
24 best practices, to measure the effectiveness of
25 cybersecurity best practices that are put into

1 use, and to identify sound means to achieve
2 widespread use of appropriate cybersecurity
3 best practices that have proven effective;

4 (B) multi-disciplinary, long-term, or high-
5 risk research and development (including asso-
6 ciated human resource development) to improve
7 cybersecurity; and

8 (C) the activities required under para-
9 graphs (3) and (4).

10 (2) CONDUCT OF RESEARCH AND DEVELOP-
11 MENT.—

12 (A) IN GENERAL.—Except as provided in
13 subparagraph (B), research and development
14 under subparagraphs (A) and (B) of paragraph
15 (1) shall be carried out using funds and other
16 support provided by the grantee to entities se-
17 lected by the grantee after full and open com-
18 petition among entities determined by the
19 grantee to be qualified to carry out such re-
20 search and development.

21 (B) CONDUCT BY GRANTEE.—The grantee
22 may carry out research and development re-
23 ferred to in subparagraph (A) in any fiscal year
24 using not more than 15 percent of the amount
25 dispersed to the grantee under this Act in such

1 fiscal year by the National Institute of Stand-
2 ards and Technology.

3 (3) RECOMMENDATIONS ON CYBERSECURITY
4 BEST PRACTICES.—

5 (A) RECOMMENDATIONS.—Not later than
6 18 months after the selection of the grantee
7 under this section, the grantee shall prepare a
8 report containing recommendations for appro-
9 priate cybersecurity best practices.

10 (B) UPDATES.—The grantee shall update
11 the recommendations made under subparagraph
12 (A) not less often than once every six months,
13 and may update any portion of such rec-
14 ommendations more frequently if the grantee
15 determines that circumstances so require.

16 (C) CONSIDERATIONS.—In making rec-
17 ommendations under subparagraph (A), and
18 any update of such recommendations under
19 subparagraph (B), the grantee shall—

20 (i) review the most current
21 cybersecurity best practices identified by
22 the National Institute of Standards and
23 Technology under section 3(a); and

24 (ii) consult with—

1 (I) the entities carrying out re-
2 search and development under para-
3 graph (1)(A);

4 (II) entities employing
5 cybersecurity best practices; and

6 (III) a wide range of academic,
7 private sector, and public entities.

8 (D) DISSEMINATION.—The grantee shall
9 submit the report under subparagraph (A), and
10 any update of the report under paragraph (B),
11 to the bodies and officials specified in para-
12 graph (5), and shall widely disseminate the re-
13 port, and any such update, among government
14 (including State and local government), private,
15 and academic entities.

16 (4) ACTIVITIES RELATING TO WIDESPREAD USE
17 OF CYBERSECURITY BEST PRACTICES.—

18 (A) IN GENERAL.—Not later than two
19 years after the selection of the grantee under
20 this section, the grantee shall submit to the
21 bodies and officials specified in paragraph (5) a
22 report containing—

23 (i) an assessment of the advisability of
24 requiring the contractors and grantees of

1 the Federal Government to use appropriate
2 cybersecurity best practices; and

3 (ii) recommendations for sound means
4 to achieve widespread use of appropriate
5 cybersecurity best practices that have prov-
6 en effective.

7 (B) REPORT ELEMENTS.—The report
8 under subparagraph (A) shall set forth—

9 (i) whether or not the requirement de-
10 scribed in subparagraph (A)(i) is advisable,
11 including whether the requirement would
12 impose undue or inappropriate burdens, or
13 other inefficiencies, on contractors and
14 grantees of the Federal Government;

15 (ii) if the requirement is determined
16 advisable—

17 (I) whether, and to what extent,
18 the requirement should be subject to
19 exceptions or limitations for particular
20 contractors or grantees, including the
21 types of contractors or grantees and
22 the nature of the exceptions or limita-
23 tions; and

24 (II) which cybersecurity best
25 practices should be covered by the re-

1 requirement and with what, if any, ex-
2 ceptions or limitations; and

3 (iii) any other matters that the grant-
4 ee considers appropriate.

5 (5) SPECIFIED BODIES AND OFFICIALS.—The
6 bodies and officials specified in this paragraph are
7 as follows:

8 (A) The appropriate committees of Con-
9 gress.

10 (B) The President.

11 (C) The Director of the Office of Manage-
12 ment and Budget.

13 (D) The National Institute of Standards
14 and Technology.

15 (E) The interagency entity designated by
16 the President under subsection (f)(1).

17 (h) GRANT ADMINISTRATION.—

18 (1) USE OF GRANT COMPETITION AND MANAGE-
19 MENT SYSTEMS.—The National Institute of Stand-
20 ards and Technology may permit the entity awarded
21 the grant under this section to utilize the grants
22 competition system and grants management system
23 of the National Institute of Standards and Tech-
24 nology for purposes of the efficient administration of
25 activities by the entity under subsection (g).

1 (2) RULES.—The National Institute of Stand-
2 ards and Technology shall establish any rules and
3 procedures that the National Institute of Standards
4 and Technology considers appropriate to further the
5 purposes of this section. Such rules may include pro-
6 visions relating to the ownership of any intellectual
7 property created by the entity awarded the grant
8 under this section or funded by the entity under
9 subsection (g).

10 (i) SUPPLEMENT NOT SUPPLANT.—The National In-
11 stitute of Standards and Technology shall take appro-
12 priate actions to ensure that activities under this section
13 supplement, rather than supplant, other current govern-
14 mental and nongovernmental efforts to protect the infor-
15 mation infrastructure of the United States.

16 **SEC. 3. APPROPRIATE CYBERSECURITY BEST PRACTICES**
17 **FOR THE FEDERAL GOVERNMENT.**

18 (a) NIST RECOMMENDATIONS.—

19 (1) IN GENERAL.—Not later than 180 days
20 after the date of the enactment of this Act, the Na-
21 tional Institute of Standards and Technology shall
22 submit to the bodies and officials specified in sub-
23 section (e) a report that—

24 (A) identifies appropriate cybersecurity
25 best practices that could reasonably be adopted

1 by the departments and agencies of the Federal
2 Government over the 24-month period begin-
3 ning on the date of the report; and

4 (B) sets forth proposed demonstration
5 projects for the adoption of such best practices
6 by various departments and agencies of the
7 Federal Government beginning 90 days after
8 the date of the report.

9 (2) UPDATES.—The National Institute of
10 Standards and Technology may submit to the bodies
11 and officials specified in subsection (e) any updates
12 of the report under paragraph (1) that the National
13 Institute of Standards and Technology consider ap-
14 propriate due to changes in circumstances.

15 (3) CONSULTATION.—In preparing the report
16 under paragraph (1), and any updates of the report
17 under paragraph (2), the National Institute of
18 Standards and Technology shall consult with depart-
19 ments and agencies of the Federal Government hav-
20 ing an interest in the report and such updates, and
21 with academic centers of expertise in cybersecurity
22 and private sector centers of expertise in
23 cybersecurity.

24 (b) DEMONSTRATION PROJECTS FOR IMPLEMENTA-
25 TION OF RECOMMENDATIONS.—

1 (1) IN GENERAL.—Commencing not later than
2 90 days after receipt of the report under subsection
3 (a), the President shall carry out the demonstration
4 projects set forth in the report, including any modi-
5 fication of any such demonstration project that the
6 President considers appropriate.

7 (2) UPDATES.—If the National Institute of
8 Standards and Technology updates under subsection
9 (a)(2) any recommendation under subsection
10 (a)(1)(A) that is relevant to a demonstration project
11 under paragraph (1), the President shall modify the
12 demonstration project to take into account such up-
13 date.

14 (3) REPORT.—Not later than nine months after
15 commencement of the demonstration projects under
16 this subsection, the President shall submit to the ap-
17 propriate committees of Congress a report on the
18 demonstration projects. The report shall set forth
19 the following:

20 (A) An assessment of the extent to which
21 the adoption of appropriate cybersecurity best
22 practices by departments and agencies of the
23 Federal Government under the demonstration
24 projects has improved cybersecurity at such de-
25 partments and agencies.

1 (B) An assessment whether or not the
2 adoption of appropriate cybersecurity best prac-
3 tices by departments and agencies of the Fed-
4 eral Government under the demonstration
5 projects has affected the capability of such de-
6 partments and agencies to carry out their mis-
7 sions.

8 (C) A description of the cost of the adop-
9 tion of appropriate cybersecurity best practices
10 by departments and agencies of the Federal
11 Government under the demonstration projects.

12 (D) A description of a security-enhancing,
13 missions-compatible, cost-effective program, to
14 the extent such program is feasible, for the
15 adoption of appropriate cybersecurity best prac-
16 tices government-wide.

17 (E) Any other matters that the President
18 considers appropriate.

19 (c) ADOPTION OF CYBERSECURITY BEST PRACTICES
20 GOVERNMENT-WIDE.—The President shall implement a
21 program for the adoption of appropriate cybersecurity best
22 practices government-wide commencing not later than six
23 months after the date of the report.

24 (d) INCORPORATION OF RECOMMENDATIONS.—If
25 during the development or implementation of the program

1 under subsection (c) the President receives any rec-
 2 ommendations under paragraph (3) or (4) of section 3(g),
 3 the President shall modify the program in order to take
 4 into account such recommendations.

5 (e) SPECIFIED BODIES AND OFFICIALS.—The bodies
 6 and officials specified in this subsection are as follows:

7 (1) The appropriate committees of Congress.

8 (2) The President.

9 (3) The Director of the Office of Management
 10 and Budget.

11 (4) The interagency entity designated by the
 12 President under section 3(f)(1).

13 **SEC. 4. DEFINITIONS.**

14 In this Act:

15 (1) APPROPRIATE COMMITTEES OF CON-
 16 GRESS.—The term “appropriate committees of Con-
 17 gress” means—

18 (A) the Committee on Commerce, Science,
 19 and Transportation of the Senate; and

20 (B) the Committee on Science of the
 21 House of Representatives.

22 (2) CYBERSECURITY.—The term
 23 “cybersecurity” means information assurance, in-
 24 cluding information security, information technology
 25 disaster recovery, and information privacy.

1 (3) CYBERSECURITY BEST PRACTICE.—The
2 term “cybersecurity best practice” means a com-
3 puter hardware or software configuration, informa-
4 tion system design, operational procedure, or meas-
5 ure, structure, or method that most effectively pro-
6 tects computer hardware, software, networks, or net-
7 work elements against an attack that would cause
8 harm through the installation of unauthorized com-
9 puter software, saturation of network traffic, alter-
10 ation of data, disclosure of confidential information,
11 or other means.

12 (4) APPROPRIATE CYBERSECURITY BEST PRAC-
13 TICE.—The term “appropriate cybersecurity best prac-
14 tice” means a cybersecurity best practice that—

15 (A) permits, as needed, customization or
16 expansion for the computer hardware, software,
17 network, or network element to which the best
18 practice applies;

19 (B) takes into account the need for secu-
20 rity protection that balances—

21 (i) the risk and magnitude of harm
22 threatened by potential attack; and

23 (ii) the cost of imposing security pro-
24 tection; and

1 (C) takes into account the rapidly chang-
2 ing nature of computer technology.

3 **SEC. 5. AUTHORIZATION OF APPROPRIATIONS.**

4 There is hereby authorized to be appropriated for the
5 National Institute of Standards and Technology for pur-
6 poses of activities under this Act, amounts as follows:

7 (1) For fiscal year 2003, \$70,000,000.

8 (2) For each of the fiscal years 2004 through
9 2007, such sums as may be necessary.

○