

107TH CONGRESS
2^D SESSION

S. 1901

To authorize the National Science Foundation and the National Security Agency to establish programs to increase the number of qualified faculty teaching advanced courses and conducting research in the field of cybersecurity, 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 Health, Education, Labor, and Pensions

A BILL

To authorize the National Science Foundation and the National Security Agency to establish programs to increase the number of qualified faculty teaching advanced courses and conducting research in the field of cybersecurity, 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 “Cybersecurity Re-
5 search and Education Act of 2002”.

6 **SEC. 2. FINDINGS.**

7 Congress finds that—

1 (1) critical elements of the Nation’s basic eco-
2 nomic and physical infrastructure rely on informa-
3 tion technology for effective functioning;

4 (2) increased reliance on technology has left our
5 Nation vulnerable to the threat of cyberterrorism;

6 (3) long-term research on practices, methods,
7 and technologies that will help ensure the safety of
8 our information infrastructure remains woefully in-
9 adequate;

10 (4) there is a critical shortage of faculty at in-
11 stitutions of higher education who specialize in dis-
12 ciplines related to cybersecurity;

13 (5) a vigorous scholarly community in fields re-
14 lated to cybersecurity is necessary to help conduct
15 research and disseminate knowledge about the prac-
16 tical application of the community’s findings; and

17 (6) universities in the United States award the
18 Ph.D. degree in computer sciences to approximately
19 1,000 individuals each year, but of those awarded
20 this degree, less than 0.3 percent specialize in
21 cybersecurity and still fewer become employed in fac-
22 ulty positions at institutions of higher education.

23 **SEC. 3. DEFINITIONS.**

24 In this Act:

1 (1) CYBERSECURITY.—The term
2 “cybersecurity” means information assurance, in-
3 cluding scientific, technical, management, or any
4 other relevant disciplines required to ensure com-
5 puter and network security, including, but not lim-
6 ited to, a discipline related to the following func-
7 tions:

8 (A) Secure system and network adminis-
9 tration and operations.

10 (B) Systems security engineering.

11 (C) Information assurance systems and
12 product acquisition.

13 (D) Cryptography.

14 (E) Threat and vulnerability assessment,
15 including risk management.

16 (F) Web security.

17 (G) Operations of computer emergency re-
18 sponse teams.

19 (H) Cybersecurity training, education, and
20 management.

21 (I) Computer forensics.

22 (J) Defensive information operations.

23 (2) CYBERSECURITY INFRASTRUCTURE.—The
24 term “cybersecurity infrastructure” includes—

1 (A) equipment that is integral to research
2 and education capabilities in cybersecurity, in-
3 cluding, but not limited to—

4 (i) encryption devices;

5 (ii) network switches;

6 (iii) routers;

7 (iv) firewalls;

8 (v) wireless networking gear;

9 (vi) protocol analyzers;

10 (vii) file servers;

11 (viii) workstations;

12 (ix) biometric tools; and

13 (x) computers; and

14 (B) technology support staff (including
15 graduate students) that is integral to research
16 and education capabilities in cybersecurity.

17 (3) DIRECTOR.—The term “Director” means
18 the Director of the National Science Foundation.

19 (4) INSTITUTION OF HIGHER EDUCATION.—The
20 term “institution of higher education” has the
21 meaning given the term in section 101(a) of the
22 Higher Education Act of 1965 (20 U.S.C. 1001(a)).

23 (5) OTHER RELEVANT DISCIPLINE.—The term
24 “other relevant discipline” includes, but is not lim-

1 ited to, the following fields as the fields specifically
2 relate to securing information infrastructures:

3 (A) Biometrics.

4 (B) Software engineering.

5 (C) Computer science and engineering.

6 (D) Law.

7 (E) Business management or administra-
8 tion.

9 (F) Psychology.

10 (G) Mathematics.

11 (H) Sociology.

12 (6) QUALIFIED INSTITUTION.—The term
13 “qualified institution” means an institution of high-
14 er education that, at the time of submission of an
15 application pursuant to any of the programs author-
16 ized by this Act—

17 (A) has offered, for not less than 3 years
18 prior to the date the application is submitted
19 under this Act, a minimum of 2 graduate
20 courses in cybersecurity (not including short-
21 term special seminars or 1-time classes offered
22 by visitors);

23 (B) has not less than 3 faculty members
24 who teach cybersecurity courses—

1 (i) each of whom has published not
2 less than 1 refereed cybersecurity research
3 article in a journal or through a conference
4 during the 2-year period preceding the
5 date of enactment of this Act;

6 (ii) at least 1 of whom is tenured; and

7 (iii) each of whom has demonstrated
8 active engagement in the cybersecurity
9 scholarly community during the 2-year pe-
10 riod preceding the date of enactment of
11 this Act, such as serving as an editor of a
12 cybersecurity journal or participating on a
13 program committee for a cybersecurity
14 conference or workshop;

15 (C) has graduated not less than 1 Ph.D.
16 scholar in cybersecurity during the 2-year pe-
17 riod preceding the date of enactment of this
18 Act; and

19 (D) has not less than 3 graduate students
20 enrolled who are pursuing a Ph.D. in
21 cybersecurity.

22 **SEC. 4. CYBERSECURITY GRADUATE FELLOWSHIP PRO-**
23 **GRAM.**

24 (a) **PURPOSE.**—The purpose of this section is—

1 (1) to encourage individuals to pursue academic
2 careers in cybersecurity upon the completion of doc-
3 toral degrees; and

4 (2) to stimulate advanced study and research,
5 at the doctoral level, in complex, relevant, and im-
6 portant issues in cybersecurity.

7 (b) ESTABLISHMENT.—The Director is authorized to
8 establish a Cybersecurity Fellowship Program (referred to
9 in this section as the “fellowship program”) to annually
10 award 3 to 5-year graduate fellowships to individuals for
11 studies and research at the doctoral level in cybersecurity.

12 (c) CYBERSECURITY FELLOWSHIP PROGRAM ADVI-
13 SORY BOARD.—

14 (1) ESTABLISHMENT.—There is established a
15 Cybersecurity Fellowship Program Advisory Board
16 (referred to in this section as the “Board”).

17 (2) MEMBERSHIP.—The Director shall appoint
18 members of the Board who shall include—

19 (A) not fewer than 3 full-time faculty
20 members—

21 (i) each of whom teaches at an insti-
22 tution of higher education; and

23 (ii) each of whom has a specialty in
24 cybersecurity; and

1 (B) not fewer than 2 research scientists
2 employed by a Federal agency with duties that
3 include cybersecurity activities.

4 (3) TERMS.—Members of the Board shall be
5 appointed for renewable 2-year terms.

6 (d) APPLICATION.—Each individual desiring to re-
7 ceive a graduate fellowship under this section shall submit
8 an application to the Director at such time, in such man-
9 ner, and containing such information as the Director, in
10 consultation with the Board, shall require.

11 (e) AWARD.—The Director is authorized to award
12 graduate fellowships under the fellowship program that
13 shall—

14 (1) be made available to individuals, through a
15 competitive selection process, for study at a qualified
16 institution and in accordance with the procedures es-
17 tablished in subsection (h);

18 (2) be in an amount that is sufficient to cover
19 annual tuition and fees for doctoral study at a quali-
20 fied institution for the duration of the graduate fel-
21 lowship, and shall include, in addition, an annual liv-
22 ing stipend of \$20,000; and

23 (3) be for a duration of 3 to 5 years, the spe-
24 cific duration of each graduate fellowship to be de-

1 terminated by the Director in consultation with the
2 Board on a case-by-case basis.

3 (f) REPAYMENT.—Each graduate fellowship shall—

4 (1) subject to paragraph (f)(2), be subject to
5 full repayment upon completion of the doctoral de-
6 gree according to a repayment schedule established
7 and administered by the Director;

8 (2) be forgiven at the rate of 20 percent of the
9 total amount of graduate fellowship assistance re-
10 ceived under this section for each academic year that
11 a recipient is employed as a full-time faculty member
12 at an institution of higher education for a period not
13 to exceed 5 years; and

14 (3) be monitored by the Director to ensure com-
15 pliance with this section.

16 (g) ELIGIBILITY.—To be eligible to receive a grad-
17 uate fellowship under this section, an individual shall—

18 (1) be a citizen of the United States;

19 (2) be matriculated or eligible to be matricu-
20 lated for doctoral studies at a qualified institution;
21 and

22 (3) demonstrate a commitment to a career in
23 higher education.

24 (h) SELECTION.—

1 (1) IN GENERAL.—The Director, in consulta-
2 tion with the Board, shall select recipients for grad-
3 uate fellowships.

4 (2) DUTIES.—The Director, in consultation
5 with the Board, shall—

6 (A) establish criteria for a competitive se-
7 lection process for recipients of graduate fellow-
8 ships;

9 (B) establish and promulgate an applica-
10 tion process for the fellowship program;

11 (C) receive applications for graduate fel-
12 lowships;

13 (D) annually review applications and select
14 recipients of graduate fellowships; and

15 (E) establish and administer a repayment
16 schedule for recipients of graduate fellowships.

17 (3) CONSIDERATION.—In making selections for
18 graduate fellowships, the Director, to the extent pos-
19 sible and in consultation with the Board, shall con-
20 sider applicants whose interests are of an inter-
21 disciplinary nature, encompassing the social sci-
22 entific as well as technical dimensions of
23 cybersecurity.

24 (i) AUTHORIZATION OF APPROPRIATIONS.—There
25 are authorized to be appropriated to carry out this section

1 \$5,000,000 for each of fiscal years 2003 through 2005,
2 and such sums as may be necessary for each succeeding
3 fiscal year.

4 **SEC. 5. SABBATICAL FOR DISTINGUISHED FACULTY IN**
5 **CYBERSECURITY.**

6 (a) ESTABLISHMENT.—The Director is authorized to
7 award grants to institutions of higher education to enable
8 faculty members who are teaching cybersecurity subjects
9 to spend a sabbatical from teaching working at—

10 (1) the National Security Agency;

11 (2) the Department of Defense;

12 (3) the National Institute of Standards and
13 Technology;

14 (4) a research laboratory supported by the De-
15 partment of Energy; or

16 (5) a qualified institution.

17 (b) APPLICATION.—Each institution of higher edu-
18 cation desiring to receive a grant under this section shall
19 submit an application to the Director at such time, in such
20 manner, and containing such information as the Director
21 shall require.

22 (c) GRANT AWARDS.—

23 (1) IN GENERAL.—The Director shall award a
24 grant under this section only if the National Science
25 Foundation and the agency or institution where the

1 faculty member will spend the sabbatical approve the
2 sabbatical placement.

3 (2) NUMBER AND DURATION.—For each fiscal
4 year, the Director shall award grants for not more
5 than 25 sabbatical positions that will each be for a
6 1-year period.

7 (3) AMOUNT OF AWARD.—

8 (A) IN GENERAL.—Each institution of
9 higher education that is awarded a grant under
10 this section shall receive \$250,000 for each fac-
11 ulty member who will spend a sabbatical pursu-
12 ant to the grant.

13 (B) USE OF AWARD.—The Director shall
14 award a grant under this section in 2 disburse-
15 ments in the following manner:

16 (i) FIRST DISBURSEMENT.—The first
17 disbursement shall be made upon selection
18 of a grant recipient and shall consist of the
19 following:

20 (I) \$20,000 to provide a stipend
21 for living expenses to each faculty
22 member awarded a sabbatical under
23 this section.

24 (II) An amount sufficient for the
25 grant recipient to hire a qualified re-

1 placement for the faculty member
2 awarded a sabbatical under this sec-
3 tion for the term of the sabbatical, if
4 such a replacement is possible.

5 (ii) SECOND DISBURSEMENT.—The
6 second disbursement shall be made at the
7 conclusion of the sabbatical, only if the
8 faculty member completes the sabbatical in
9 its entirety, and shall be used for the grant
10 recipient's cybersecurity infrastructure
11 needs, including—

12 (I) acquiring equipment or tech-
13 nology;

14 (II) hiring graduate students; or

15 (III) supporting any other activ-
16 ity that will enhance the grant recipi-
17 ent's course offerings and research in
18 cybersecurity.

19 (d) ELIGIBILITY.—To be eligible to receive a grant
20 under this section, an institution of higher education shall
21 submit an application under subsection (b) that—

22 (1) identifies the faculty member to whom the
23 institution of higher education will provide a sab-
24 batical and ensures that the faculty member is a cit-
25 izen of the United States;

1 (2) ensures that the faculty member to whom
2 the institution of higher education will provide a
3 sabbatical is tenured at that institution of higher
4 education and meets general standards of excellence
5 in research or teaching; and

6 (3) explains how the faculty member to whom
7 the institution of higher education will provide a
8 sabbatical will—

9 (A) integrate into the faculty member's
10 course offerings knowledge related to
11 cybersecurity that is gained during the sab-
12 batical; and

13 (B) in conjunction with the institution of
14 higher education, use the second disbursement
15 of funds available under subsection
16 (c)(3)(B)(ii).

17 (e) AUTHORIZATION OF APPROPRIATIONS.—There is
18 authorized to be appropriated to carry out this section
19 \$8,000,000 for each of fiscal years 2003 through 2005.

20 **SEC. 6. ENHANCING CYBERSECURITY INFRASTRUCTURE.**

21 (a) ESTABLISHMENT.—The Director is authorized to
22 award grants to qualified institutions to fund activities
23 that provide, enhance, and facilitate acquisition of
24 cybersecurity infrastructure at qualified institutions.

1 (b) USE OF GRANT AWARD.—Each qualified institu-
2 tion that receives a grant under this section shall use the
3 grant funds for needs specifically related to—

4 (1) cybersecurity education and research; and

5 (2) development efforts related to cybersecurity.

6 (c) MATCHING FUNDS.—Each qualified institution
7 that receives a grant under this section shall contribute
8 to the activities assisted under this section non-Federal
9 matching funds equal to not less than 25 percent of the
10 amount of the grant.

11 (d) AUTHORIZATION OF APPROPRIATIONS.—There is
12 authorized to be appropriated to carry out this section
13 \$10,000,000 for each of fiscal years 2003 through 2005.

14 **SEC. 7. CYBERSECURITY AWARENESS, TRAINING, AND EDU-**
15 **CATION PROGRAM.**

16 (a) PURPOSE.—The purpose of this section is to in-
17 crease the quality of education and training in
18 cybersecurity, thereby increasing the number of qualified
19 students entering the field of cybersecurity to adequately
20 address the Nation's increasing dependence on informa-
21 tion technology and to defend the Nation's increasingly
22 vulnerable information infrastructure.

23 (b) ESTABLISHMENT.—The Director of the National
24 Security Agency is authorized to award grants, on a com-
25 petitive basis, to qualified institutions to establish

1 Cybersecurity Awareness, Training, and Education Pro-
2 grams (referred to in this section as “information pro-
3 grams”).

4 (c) APPLICATION.—

5 (1) IN GENERAL.—Each qualified institution
6 desiring to receive a grant under this section shall
7 submit an application to the Director of the Na-
8 tional Security Agency at such time, in such man-
9 ner, and accompanied by such information as the
10 Director of the National Security Agency shall re-
11 quire.

12 (2) PLANS.—Each application submitted pursu-
13 ant to paragraph (1) shall include a plan for estab-
14 lishing and maintaining an information program
15 under this section, including a description of—

16 (A) the design, structure, and scope of the
17 proposed information program, including unique
18 qualities that may distinguish the proposed in-
19 formation program from possible approaches of
20 other qualified institutions;

21 (B) research being conducted in the dis-
22 ciplines encompassed by the plan;

23 (C) any integration of the information pro-
24 gram with other federally funded programs re-
25 lated to cybersecurity education, such as the

1 National Science Foundation Scholarship for
2 Service Program, the Department of Defense
3 Multidisciplinary Research Program of the Uni-
4 versity Research Initiative, and the Department
5 of Defense Information Assurance Scholarship
6 Program;

7 (D) necessary costs for information infra-
8 structure to support the information program;

9 (E) how the qualified institution will pro-
10 tect the integrity and security of the informa-
11 tion infrastructure and any student testing
12 mechanisms; and

13 (F) other relevant information.

14 (3) COLLABORATION.—A qualified institution
15 desiring to receive a grant under this section may
16 propose collaboration with other qualified institu-
17 tions.

18 (d) GRANT AWARDS.—Each qualified institution that
19 receives a grant under this section shall use the grant
20 funds to—

21 (1) establish or enhance a Center for Studies in
22 Cybersecurity Awareness, Training, and Education
23 that shall—

24 (A) establish a professionally produced,
25 web-based collection of cybersecurity programs

1 of instruction that have been approved for gen-
2 eral public dissemination by the authors and
3 owners of the programs;

4 (B) maintain a web-based directory of
5 cybersecurity education and training related
6 conferences and symposia;

7 (C) sponsor the development of specific in-
8 structional materials in cybersecurity and other
9 relevant disciplines, including—

10 (i) intrusion detection;

11 (ii) overview of information assurance;

12 (iii) ethical use of computing systems;

13 (iv) network security;

14 (v) cryptography;

15 (vi) risk management;

16 (vii) malicious logic; and

17 (viii) system security engineering;

18 (D) sponsor cybersecurity education
19 symposia;

20 (E) collaborate with the National
21 Colloquium for Information Assurance Edu-
22 cation;

23 (F) create a “Virtual Academy” for shar-
24 ing courseware and laboratory exercises in
25 cybersecurity; and

1 (G) review and participate in integrating
2 various cybersecurity education and training
3 standards into unified curricula; and

4 (2) establish or enhance a Center for the Devel-
5 opment of Faculty in Cybersecurity that shall—

6 (A) establish criteria for recognition and
7 certification of cybersecurity trainers and edu-
8 cators;

9 (B) establish faculty training outreach to
10 teachers in kindergarten through grade 12 and
11 to faculty of part B institutions (as defined in
12 section 322 of the Higher Education Act of
13 1965 (20 U.S.C. 1061));

14 (C) build, test, and evaluate laboratory ex-
15 ercises that represent use of model practices in
16 cybersecurity for use in training and education
17 programs; and

18 (D) establish an integrated program to in-
19 clude the programs described in this paragraph
20 and paragraph (1).

21 (e) AUTHORIZATION OF APPROPRIATIONS.—There
22 are authorized to be appropriated to carry out this
23 section—

24 (1) \$1,500,000 for fiscal year 2003;

25 (2) \$2,000,000 for fiscal year 2004;

1 (3) \$3,000,000 for fiscal year 2005; and

2 (4) \$4,500,000 for fiscal year 2006.

3 **SEC. 8. CYBERSECURITY WORKFORCE AND FACILITIES**

4 **STUDY.**

5 (a) STUDY.—The Comptroller General shall conduct
6 a study and collect data on the following:

7 (1) The cybersecurity workforce, including—

8 (A) the size and nature of the
9 cybersecurity workforce by occupation category
10 (including academic faculty at institutions of
11 higher education), level of education and train-
12 ing, personnel demographics, and industry char-
13 acteristics; and

14 (B) the role of foreign workers in the
15 cybersecurity workforce.

16 (2) Academic cybersecurity research facilities,
17 including—

18 (A) total academic research space available
19 or utilized for research relating to
20 cybersecurity;

21 (B) academic research space relating to
22 cybersecurity that is in need of major repair or
23 renovation;

24 (C) new or ongoing projects at institutions
25 of higher education expected to produce new or

1 renovated research space to be used for re-
2 search relating to cybersecurity; and

3 (D) any research space needs related to
4 cybersecurity and based on projections of
5 growth in educational programs and research,
6 including costs and initiatives required to meet
7 such needs and possible consequences of failure
8 to meet such needs.

9 (3) Other information that the Comptroller
10 General determines appropriate.

11 (b) REPORT.—Not later than 6 months after the date
12 of enactment of this Act, and biennially thereafter, the
13 Comptroller General shall prepare and submit a report on
14 the study conducted pursuant to subsection (a) to the—

15 (1) Committee on Health, Education, Labor
16 and Pensions of the Senate; and

17 (2) Committee on Education and the Workforce
18 of the House of Representatives.

○