(C) the capacity of the applicant to attract and provide adequate support for a diverse group of undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research;

(D) the extent to which the applicant will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions, and the role the partners will play in the research undertaken by the Center;

(E) the demonstrated capability of the applicant to conduct high performance computation integral to complex computer and network security research, through on-site or off-site computing;

(F) the applicant's affiliation with private sector entities involved with industrial research described in subsection (a)(1);

(G) the capability of the applicant to conduct research in a secure environment;

(H) the applicant's affiliation with existing research programs of the Federal Government;

(I) the applicant's experience managing public-private partnerships to transition new technologies into a commercial setting or the government user community;

(J) the capability of the applicant to conduct interdisciplinary cybersecurity research, basic and applied, such as in law, economics, or behavioral sciences; and

(K) the capability of the applicant to conduct research in areas such as systems security, wireless security, networking and protocols, formal methods and high-performance computing, nanotechnology, or industrial control systems.

(6) Annual meeting

The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) Authorization of appropriations

There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;

(B) $24,000,000 for fiscal year 2004;

(C) $36,000,000 for fiscal year 2005;

(D) $36,000,000 for fiscal year 2006; and

(E) $36,000,000 for fiscal year 2007.

(Pub. L. 107–305, § 4, Nov. 27, 2002, 116 Stat. 2368; Pub. L. 113–274, title II, §§ 201(e), 202, Dec. 18, 2014, 128 Stat. 2978.)

AMENDMENTS

2014—Subsec. (a)(1)(J) to (P). Pub. L. 113–274, § 201(e), added subpars. (J) to (P).

Subsec. (b)(3). Pub. L. 113–274, § 202(1), substituted ''improving the security and resiliency of information technology, reducing cyber vulnerabilities, and anticipating and mitigating consequences of cyber attacks on critical infrastructure, by conducting research in the areas'' for ''the research areas''.

Subsec. (b)(4)(D). Pub. L. 113–274, § 202(2), substituted ''the Center'' for ''the center''.

Subsec. (b)(5)(E) to (K). Pub. L. 113–274, § 202(3), added subpars. (E) to (K).

§ 7404. National Science Foundation computer and network security programs

(a) Computer and network security capacity building grants

(1) In general

The Director shall establish a program to award grants to institutions of higher education (or consortia thereof) to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students, including the number of students from groups historically underrepresented in these fields, who pursue undergraduate or master's degrees in fields related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies.

(2) Merit review

Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) Use of funds

Grants awarded under this subsection shall be used for activities that enhance the ability of an institution of higher education (or consortium thereof) to provide high-quality undergraduate and master's degree programs in computer and network security and to recruit and retain increased numbers of students to such programs. Activities may include—

(A) revising curriculum to better prepare undergraduate and master's degree students for careers in computer and network security;

(B) establishing degree and certificate programs in computer and network security;

(C) creating opportunities for undergraduate students to participate in computer and network security research projects;

(D) acquiring equipment necessary for student instruction in computer and network security, including the installation of testbed networks for student use;

(E) providing opportunities for faculty to work with local or Federal Government agencies, private industry, nonprofit research institutions, or other academic institutions to develop new expertise or to formulate new research directions in computer and network security;

(F) establishing collaborations with other academic institutions or academic departments that seek to establish, expand, or enhance programs in computer and network security;

(G) establishing student internships in computer and network security at government agencies or in private industry;

(H) establishing collaborations with other academic institutions to establish or enhance a web-based collection of computer and network security courseware and laboratory exercises for sharing with other institutions of higher education, including community colleges;

(I) establishing or enhancing bridge programs in computer and network security between community colleges and universities; and

(J) any other activities the Director determines will accomplish the goals of this subsection.

(4) Selection process

(A) Application

An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum—

(i) a description of the applicant's computer and network security research and instructional capacity, and in the case of an application from a consortium of institutions of higher education, a description of the role that each member will play in implementing the proposal;

(ii) a comprehensive plan by which the institution or consortium will build instructional capacity in computer and information security;

(iii) a description of relevant collaborations with government agencies or private industry that inform the instructional program in computer and network security;

(iv) a survey of the applicant's historic student enrollment and placement data in fields related to computer and network security and a study of potential enrollment and placement for students enrolled in the proposed computer and network security program; and

(v) a plan to evaluate the success of the proposed computer and network security program, including post-graduation assessment of graduate school and job placement and retention rates as well as the relevance of the instructional program to graduate study and to the workplace.

(B) Awards

(i) The Director shall ensure, to the extent practicable, that grants are awarded under this subsection in a wide range of geographic areas and categories of institutions of higher education, including minority serving institutions.

(ii) The Director shall award grants under this subsection for a period not to exceed 5 years.

(5) Assessment required

The Director shall evaluate the program established under this subsection no later than 6 years after the establishment of the program. At a minimum, the Director shall evaluate the extent to which the program achieved its objectives of increasing the quality and quantity of students, including students from groups historically underrepresented in computer and network security related disciplines, pursuing undergraduate or master's degrees in computer and network security.

(6) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $15,000,000 for fiscal year 2003;
(B) $20,000,000 for fiscal year 2004;
(C) $20,000,000 for fiscal year 2005;
(D) $20,000,000 for fiscal year 2006; and
(E) $20,000,000 for fiscal year 2007.

(b) Scientific and Advanced Technology Act of 1992

(1) Grants

The Director shall provide grants under the Scientific and Advanced Technology Act of 1992 (42 U.S.C. 1862i) [42 U.S.C. 1862h et seq.] for the purposes of section 3(a) and (b) of that Act [42 U.S.C. 1862i(a), (b)], except that the activities supported pursuant to this subsection shall be limited to improving education in fields related to computer and network security.

(2) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $1,000,000 for fiscal year 2003;
(B) $1,250,000 for fiscal year 2004;
(C) $1,250,000 for fiscal year 2005;
(D) $1,250,000 for fiscal year 2006; and
(E) $1,250,000 for fiscal year 2007.

(c) Graduate traineeships in computer and network security research

(1) In general

The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs for graduate students who pursue computer and network security research leading to a doctorate degree by providing funding and other assistance, and by providing graduate students with research experience in government or industry related to the students' computer and network security studies.

(2) Merit review

Grants shall be provided under this subsection on a merit-reviewed competitive basis.

(3) Use of funds

An institution of higher education shall use grant funds for the purposes of—

(A) providing traineeships to students who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are pursuing research in computer or network security leading to a doctorate degree;

(B) paying tuition and fees for students receiving traineeships under subparagraph (A);

(C) establishing scientific internship programs for students receiving traineeships under subparagraph (A) in computer and network security at for-profit institutions, nonprofit research institutions, or government laboratories; and

(D) other costs associated with the administration of the program.

(4) Traineeship amount

Traineeships provided under paragraph (3)(A) shall be in the amount of $25,000 per year, or the level of the National Science Foundation Graduate Research Fellowships, whichever is greater, for up to 3 years.

(5) Selection process

An institution of higher education seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the instructional program and research opportunities in computer and network security available to graduate students at the applicant's institution; and

(B) the internship program to be established, including the opportunities that will be made available to students for internships at for-profit institutions, nonprofit research institutions, and government laboratories.

(6) Review of applications

In evaluating the applications submitted under paragraph (5), the Director shall consider—

(A) the ability of the applicant to effectively carry out the proposed program;

(B) the quality of the applicant's existing research and education programs;

(C) the likelihood that the program will recruit increased numbers of students, including students from groups historically underrepresented in computer and network security related disciplines, to pursue and earn doctorate degrees in computer and network security;

(D) the nature and quality of the internship program established through collaborations with government laboratories, nonprofit research institutions, and for-profit institutions;

(E) the integration of internship opportunities into graduate students' research; and

(F) the relevance of the proposed program to current and future computer and network security needs.

(7) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $10,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(d) Graduate Research Fellowships program support

Computer and network security shall be included among the fields of specialization supported by the National Science Foundation's Graduate Research Fellowships program under section 1869 of title 42.

(e) Cyber security faculty development traineeship program

(1) In general

The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees.

(2) Merit review; competition

Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) Application

Each institution of higher education desiring to receive a grant under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director shall require.

(4) Use of funds

Funds received by an institution of higher education under this paragraph shall—

(A) be made available to individuals on a merit-reviewed competitive basis and in accordance with the requirements established in paragraph (7);

(B) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at an institution of higher education for the duration of the graduate traineeship, and shall include, in addition, an annual living stipend of $25,000; and

(C) be provided to individuals for a duration of no more than 5 years, the specific duration of each graduate traineeship to be determined by the institution of higher education, on a case-by-case basis.

(5) Repayment

Each graduate traineeship shall—

(A) subject to paragraph (5)(B), be subject to full repayment upon completion of the doctoral degree according to a repayment schedule established and administered by the institution of higher education;

(B) be forgiven at the rate of 20 percent of the total amount of the graduate traineeship assistance received under this section for each academic year that a recipient is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

(C) be monitored by the institution of higher education receiving a grant under this subsection to ensure compliance with this subsection.

(6) Exceptions

The Director may provide for the partial or total waiver or suspension of any service obligation or payment by an individual under this section whenever compliance by the individual is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(7) Eligibility

To be eligible to receive a graduate traineeship under this section, an individual shall—

(A) be a citizen, national, or lawfully admitted permanent resident alien of the United States; and

(B) demonstrate a commitment to a career in higher education.

(8) Consideration

In making selections for graduate traineeships under this paragraph, an institution receiving a grant under this subsection shall consider, to the extent possible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security.

(9) Authorization of appropriations

There are authorized to be appropriated to the National Science Foundation to carry out this paragraph $5,000,000 for each of fiscal years 2003 through 2007.

(Pub. L. 107–305, § 5, Nov. 27, 2002, 116 Stat. 2370.)

REFERENCES IN TEXT

The Scientific and Advanced Technology Act of 1992, referred to in subsec. (b)(1), is Pub. L. 102–476, Oct. 23, 1992, 106 Stat. 2297, as amended, which is classified generally to section 1862h et seq. of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 1861 of Title 42 and Tables.

§ 7405. Consultation

In carrying out sections 7403 and 7404 of this title, the Director shall consult with other Federal agencies.

(Pub. L. 107–305, § 6, Nov. 27, 2002, 116 Stat. 2374.)

§ 7406. National Institute of Standards and Technology programs

(a), (b) Omitted

(c) Security automation and checklists for Government systems

(1) In general

The Director of the National Institute of Standards and Technology shall, as necessary, develop and revise security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government, thereby enabling standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

(2) Priorities for development

The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

(A) the security risks associated with the use of the system;

(B) the number of agencies that use a particular system or security tool;

(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

(3) Excluded systems

The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the lack of utility or impracticability of developing a standard, reference material, or checklist for the system.

(4) Dissemination of standards and related materials

The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

(5) Agency use requirements

The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed or identified under paragraph (1).

(d) Federal agency information security programs

(1) In general

In developing the agencywide information security program required by section 3554(b) of title 44, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) shall include in that program an explanation of how the agency has considered such checklist in deploying that system; and

(B) may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31).

(2) Limitation

Paragraph (1) does not apply to any computer hardware or software system for which the National Institute of Standards and Technology does not have responsibility under section 278g–3(a)(3) of this title.

(Pub. L. 107–305, § 8, Nov. 27, 2002, 116 Stat. 2375; Pub. L. 113–274, title II, § 203, Dec. 18, 2014, 128 Stat. 2979; Pub. L. 113–283, § 2(e)(2), Dec. 18, 2014, 128 Stat. 3086.)

CODIFICATION

Section is comprised of section 8 of Pub. L. 107–305. Subsec. (a) of section 8 of Pub. L. 107–305 enacted sec-