munications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results ''clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure''.

(4) Computer security technology and systems implementation lack—

(A) sufficient long term research funding;

(B) adequate coordination across Federal and State government agencies and among government, academia, and industry; and

(C) sufficient numbers of outstanding researchers in the field.

(5) Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) improve vulnerability assessment and technological and systems solutions;

(B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

(C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

(6) While African-Americans, Hispanics, and Native Americans constitute 25 percent of the total United States workforce and 30 percent of the college-age population, members of these minorities comprise less than 7 percent of the United States computer and information science workforce.

(Pub. L. 107–305, § 2, Nov. 27, 2002, 116 Stat. 2367.)

SHORT TITLE

Pub. L. 107–305, § 1, Nov. 27, 2002, 116 Stat. 2367, provided that: ''This Act [enacting this chapter and section 278h of this title, amending sections 278g–3, 1511e, and 7301 of this title and section 1862 of Title 42, The Public Health and Welfare, and redesignating section 278h of this title as 278q of this title] may be cited as the 'Cyber Security Research and Development Act'.''

§ 7402. Definitions

In this chapter:

(1) Director

The term ''Director'' means the Director of the National Science Foundation.

(2) Institution of higher education

The term ''institution of higher education'' has the meaning given that term in section 1001(a) of title 20.

(Pub. L. 107–305, § 3, Nov. 27, 2002, 116 Stat. 2368.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 107–305, Nov. 27, 2002, 116 Stat. 2367, known as the Cyber Security Research and Development Act, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title and Tables.

§ 7403. National Science Foundation research

(a) Computer and network security research grants

(1) In general

The Director shall award grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication, cryptography, and other secure data communications technology;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure;

(D) privacy and confidentiality;

(E) network security architecture, including tools for security administration and analysis;

(F) emerging threats;

(G) vulnerability assessments and techniques for quantifying risk;

(H) remote access and wireless security;

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property;

(J) secure fundamental protocols that are integral to inter-network communications and data exchange;

(K) secure software engineering and software assurance, including—

(i) programming languages and systems that include fundamental security features;

(ii) portable or reusable code that remains secure when deployed in various environments;

(iii) verification and validation technologies to ensure that requirements and specifications have been implemented; and

(iv) models for comparison and metrics to assure that required standards have been met;

(L) holistic system security that—

(i) addresses the building of secure systems from trusted and untrusted components;

(ii) proactively reduces vulnerabilities;

(iii) addresses insider threats; and

(iv) supports privacy in conjunction with improved security;

(M) monitoring and detection;

(N) mitigation and rapid recovery methods;

(O) security of wireless networks and mobile devices;

(P) security of cloud infrastructure and services;

(Q) security of election-dedicated voting system software and hardware; and

(R) role of the human factor in cybersecurity and the interplay of computers and humans and the physical world.

(2) Merit review; competition

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

(3) Authorization of appropriations

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

(A) $35,000,000 for fiscal year 2003;
(B) $40,000,000 for fiscal year 2004;
(C) $46,000,000 for fiscal year 2005;
(D) $52,000,000 for fiscal year 2006; and
(E) $60,000,000 for fiscal year 2007.

(b) Computer and network security research centers

(1) In general

The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education, nonprofit research institutions, or consortia thereof to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education, nonprofit research institutions, or consortia thereof receiving such grants may partner with 1 or more government laboratories or for-profit institutions, or other institutions of higher education or nonprofit research institutions.

(2) Merit review; competition

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

(3) Purpose

The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and network security, including 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 described in subsection (a)(1).

(4) Applications

An institution of higher education, nonprofit research institution, or consortia 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, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;
(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers;
(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; and
(D) how the Center will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services.

(5) Criteria

In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;
(B) the experience of the applicant in conducting research on computer and network security and the capacity of the applicant to foster new multidisciplinary collaborations;
(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 networking and information technology, 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; Pub. L. 114–329, title I, §§104(a), 105(r), Jan. 6, 2017, 130 Stat. 2975, 2984.)

AMENDMENTS

2017—Subsec. (a)(1)(Q), (R). Pub. L. 114–329, §104(a), added subpars. (Q) and (R).

Subsec. (b)(5)(K). Pub. L. 114–329, §105(r), substituted ''networking and information technology'' for ''high-performance computing''.

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