acquire the expertise, equipment, and training necessary to participate fully in supply chains using enterprise integration.

(Pub. L. 107–277, § 3, Nov. 5, 2002, 116 Stat. 1936; Pub. L. 113–188, title II, § 201(b), Nov. 26, 2014, 128 Stat. 2018; Pub. L. 114–329, title V, § 501(e)(2), Jan. 6, 2017, 130 Stat. 3033.)

Editorial Notes

REFERENCES IN TEXT

This Act, referred to in subsec. (c), is Pub. L. 107–277, Nov. 5, 2002, 116 Stat. 1936, known as the Enterprise Integration Act of 2002, which enacted this section and provisions set out as a note under this section. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was enacted as part of the Enterprise Integration Act of 2002, and not as part of the National Institute of Standards and Technology Act which comprises this chapter.

AMENDMENTS

2017—Subsec. (a). Pub. L. 114–329 inserted ''Hollings'' before ''Manufacturing Extension Partnership''.

2014—Subsecs. (c) to (e). Pub. L. 113–188 redesignated subsecs. (d) and (e) as (c) and (d), respectively, and struck out former subsec. (c) which required annual reports on the National Institute of Standards and Technology's activities under subsec. (b).

Statutory Notes and Related Subsidiaries

ENTERPRISE INTEGRATION

Pub. L. 107–277, Nov. 5, 2002, 116 Stat. 1936, provided that:

''SECTION. 1. SHORT TITLE.

''This Act [enacting this section and this note] may be cited as the 'Enterprise Integration Act of 2002'.

''SEC. 2. FINDINGS.

''The Congress makes the following findings:

''(1) Over 90 percent of United States companies engaged in manufacturing are small- and medium-sized businesses.

''(2) Most of these manufacturers produce goods for assemblage into products of large companies.

''(3) The emergence of the World Wide Web and the promulgation of international standards for product data exchange greatly accelerated the movement toward electronically integrated supply chains during the last half of the 1990's.

''(4) European and Asian countries are investing heavily in electronic enterprise standards development, and in preparing their smaller manufacturers to do business in the new environment. European efforts are well advanced in the aerospace, automotive, and shipbuilding industries and are beginning in other industries including home building, furniture manufacturing, textiles, and apparel. This investment could give overseas companies a major competitive advantage.

''(5) The National Institute of Standards and Technology, because of the electronic commerce expertise in its laboratories and quality program, its long history of working cooperatively with manufacturers, and the nationwide reach of its manufacturing extension program, is in a unique position to help United States large and smaller manufacturers alike in their responses to this challenge.

''(6) It is, therefore, in the national interest for the National Institute of Standards and Technology to accelerate its efforts in helping industry develop standards and enterprise integration processes that are necessary to increase efficiency and lower costs.

''SEC. 3. ENTERPRISE INTEGRATION INITIATIVE.

[Enacted this section.]

''SEC. 4. DEFINITIONS.

''For purposes of this Act—

''(1) the term 'automotive' means land-based engine-powered vehicles including automobiles, trucks, busses, trains, defense vehicles, farm equipment, and motorcycles;

''(2) the term 'Director' means the Director of the National Institute of Standards and Technology;

''(3) the term 'enterprise integration' means the electronic linkage of manufacturers, assemblers, suppliers, and customers to enable the electronic exchange of product, manufacturing, and other business data among all partners in a product supply chain, and such term includes related application protocols and other related standards;

''(4) the term 'major manufacturing industry' includes the aerospace, automotive, electronics, shipbuilding, construction, home building, furniture, textile, and apparel industries and such other industries as the Director designates; and

''(5) the term 'roadmap' means an assessment of manufacturing interoperability requirements developed by an industry describing that industry's goals related to enterprise integration, the knowledge and standards including application protocols necessary to achieve those goals, and the necessary steps, timetable, and assignment of responsibilities for acquiring the knowledge and developing the standards and protocols.

''SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

''There are authorized to be appropriated to the Director to carry out functions under this Act—

''(1) $2,000,000 for fiscal year 2002;

''(2) $10,000,000 for fiscal year 2003;

''(3) $15,000,000 for fiscal year 2004; and

''(4) $20,000,000 for fiscal year 2005.''

§ 278h. Research program on security of computer systems

(a) Establishment

The Director shall establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems. The partnerships may also include government laboratories and nonprofit research institutions. The program shall—

(1) include multidisciplinary, long-term research;

(2) include research directed toward addressing needs identified through the activities of the Computer System Security[1] and Privacy Advisory Board under section 278g–3(f)[2] of this title; and

(3) promote the development of a robust research community working at the leading edge of knowledge in subject areas relevant to the security of computer systems by providing support for graduate students, post-doctoral researchers, and senior researchers.

(b) Fellowships

(1) Post-doctoral research fellowships

The Director is authorized to establish a program to award post-doctoral research fellowships to individuals who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are seek-

[1] So in original. Probably should be ''Information Security''.

[2] See References in Text note below.

ing research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 7403(a)(1) of this title.

(2) Senior research fellowships

The Director is authorized to establish a program to award senior research fellowships to individuals seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 7403(a)(1) of this title. Senior research fellowships shall be made available for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems.

(3) Eligibility

(A) In general

To be eligible for an award under this subsection, an individual shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require.

(B) Stipends

Under this subsection, the Director is authorized to provide stipends for post-doctoral research fellowships at the level of the Institute's Post Doctoral Research Fellowship Program and senior research fellowships at levels consistent with support for a faculty member in a sabbatical position.

(c) Awards; applications

(1) In general

The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a). No funds made available under this section shall be made available directly to any for-profit partners.

(2) Eligibility

To be eligible for an award under this section, an institution of higher education 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 number of graduate students anticipated to participate in the research project and the level of support to be provided to each;

(B) the number of post-doctoral research positions included under the research project and the level of support to be provided to each;

(C) the number of individuals, if any, intending to change research fields and pursue studies related to the security of computer systems to be included under the research project and the level of support to be provided to each; and

(D) how the for-profit entities, nonprofit research institutions, and any other partners will participate in developing and carrying out the research and education agenda of the partnership.

(d) Program operation

(1) Management

The program established under subsection (a) shall be managed by individuals who shall have both expertise in research related to the security of computer systems and knowledge of the vulnerabilities of existing computer systems. The Director shall designate such individuals as program managers.

(2) Managers may be employees

Program managers designated under paragraph (1) may be new or existing employees of the Institute or individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 [42 U.S.C. 4701 et seq.], except that individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 shall not directly manage such employees.

(3) Manager responsibility

Program managers designated under paragraph (1) shall be responsible for—

(A) establishing and publicizing the broad research goals for the program;

(B) soliciting applications for specific research projects to address the goals developed under subparagraph (A);

(C) selecting research projects for support under the program from among applications submitted to the Institute, following consideration of—

(i) the novelty and scientific and technical merit of the proposed projects;

(ii) the demonstrated capabilities of the individual or individuals submitting the applications to successfully carry out the proposed research;

(iii) the impact the proposed projects will have on increasing the number of computer security researchers;

(iv) the nature of the participation by for-profit entities and the extent to which the proposed projects address the concerns of industry; and

(v) other criteria determined by the Director, based on information specified for inclusion in applications under subsection (c); and

(D) monitoring the progress of research projects supported under the program.

(4) Reports

The Director shall report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science annually on the use and responsibility of individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 [42 U.S.C. 4701 et seq.] who are performing duties under subsection (d).

(e) Review of program

(1) Periodic review

The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (d). In conducting those reviews, the Director shall seek the advice of

the Computer System Security[1] and Privacy Advisory Board, established under section 278g–4 of this title, on the appropriateness of the research goals and on the quality and utility of research projects managed by program managers in accordance with subsection (d).

(2) Comprehensive 5-year review

The Director shall also contract with the National Research Council for a comprehensive review of the program established under subsection (a) during the 5th year of the program. Such review shall include an assessment of the scientific quality of the research conducted, the relevance of the research results obtained to the goals of the program established under subsection (d)(3)(A), and the progress of the program in promoting the development of a substantial academic research community working at the leading edge of knowledge in the field. The Director shall submit to Congress a report on the results of the review under this paragraph no later than 6 years after the initiation of the program.

(f) Definitions

In this section:

(1) Computer system

The term ''computer system'' has the meaning given that term in section 278g–3(d)(1)[2] of this title.

(2) Institution of higher education

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

(Mar. 3, 1901, ch. 872, § 22, as added Pub. L. 107–305, § 8(a)(2), Nov. 27, 2002, 116 Stat. 2375.)

Editorial Notes

REFERENCES IN TEXT

Section 278g–3 of this title, referred to in subsecs. (a)(2) and (f)(1), was amended generally by Pub. L. 107–296, title X, § 1003, Nov. 25, 2002, 116 Stat. 2269, and, as so amended, did not contain a subsec. (d) defining ''computer system'' or a subsec. (f). A later amendment by Pub. L. 113–274, title II, § 204(1), Dec. 18, 2014, 128 Stat. 2980, redesignated subsec. (e) of section 278g–3 of this title, relating to definitions, as subsec. (f).

The Intergovernmental Personnel Act of 1970, referred to in subsec. (d)(2), (4), is Pub. L. 91–648, Jan. 5, 1971, 84 Stat. 1909, which enacted sections 3371 to 3376 of Title 5, Government Organization and Employees, and chapter 62 (§ 4701 et seq.) of Title 42, The Public Health and Welfare, amended section 1304 of Title 5 and section 246 of Title 42, repealed sections 1881 to 1888 of Title 7, Agriculture, and section 869b of Title 20, Education, and enacted provisions set out as notes under section 3371 of Title 5. For complete classification of this Act to the Code, see Short Title note set out under section 4701 of Title 42 and Tables.

PRIOR PROVISIONS

A prior section 22 of act Mar. 3, 1901, ch. 872, was renumbered section 32 and is classified to section 278q of this title.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Science of House of Representatives changed to Committee on Science and Technology of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Science and Technology of House of Representatives changed to Committee on Science, Space, and Technology of House of Representatives by House Resolution No. 5, One Hundred Twelfth Congress, Jan. 5, 2011.

§ 278h–1. Standards for artificial intelligence

(a) Mission

The Institute shall—

(1) advance collaborative frameworks, standards, guidelines, and associated methods and techniques for artificial intelligence;

(2) support the development of a risk-mitigation framework for deploying artificial intelligence systems;

(3) support the development of technical standards and guidelines that promote trustworthy artificial intelligence systems; and

(4) support the development of technical standards and guidelines by which to test for bias in artificial intelligence training data and applications.

(b) Supporting activities

The Director of the National Institute of Standards and Technology may—

(1) support measurement research and development of best practices and voluntary standards for trustworthy artificial intelligence systems, which may include—

(A) privacy and security, including for datasets used to train or test artificial intelligence systems and software and hardware used in artificial intelligence systems;

(B) advanced computer chips and hardware designed for artificial intelligence systems;

(C) data management and techniques to increase the usability of data, including strategies to systematically clean, label, and standardize data into forms useful for training artificial intelligence systems and the use of common, open licenses;

(D) safety and robustness of artificial intelligence systems, including assurance, verification, validation, security, control, and the ability for artificial intelligence systems to withstand unexpected inputs and adversarial attacks;

(E) auditing mechanisms and benchmarks for accuracy, transparency, verifiability, and safety assurance for artificial intelligence systems;

(F) applications of machine learning and artificial intelligence systems to improve other scientific fields and engineering;

(G) model documentation, including performance metrics and constraints, measures of fairness, training and testing processes, and results;

(H) system documentation, including connections and dependences within and between systems, and complications that may arise from such connections; and

(I) all other areas deemed by the Director to be critical to the development and deployment of trustworthy artificial intelligence;

(2) produce curated, standardized, representative, high-value, secure, aggregate, and privacy protected data sets for artificial intelligence research, development, and use;

(3) support one or more institutes as described in section 9431(b) of this title for the