from among citizens, nationals, and lawfully admitted permanent resident aliens of the United States.

(c) Outreach

The Director of the National Science Foundation shall conduct program outreach to recruit fellowship applicants—

(1) from all regions of the country;

(2) from historically underrepresented populations in the fields of science, technology, engineering, and mathematics; and

(3) who graduate from or intend to carry out research at a variety of types of institutions of higher education, including—

(A) historically Black colleges and universities;

(B) Tribal Colleges and Universities;

(C) minority-serving institutions;

(D) institutions of higher education that are not among the top 50 institutions in annual Federal funding for research; and

(E) EPSCoR institutions.

(d) Special consideration

The Director of the National Science Foundation shall give special consideration and priority to an application from an individual who graduated from or is intending to carry out research at an institution of the type specified in subsection (c)(3).

(e) Reports from fellows

Not later than 180 days after the end of the pilot program under this section, each early-career investigator who receives an award under the pilot program shall submit to the Director of the National Science Foundation a report that describes how the early-career investigator used the award funds.

(f) Report from the Director

Not later than 90 days after the conclusion of the second year of the pilot program, the Director of the National Science Foundation shall submit to Congress a report that includes the following:

(1) A summary of the uses of award funds under this section and the impact of the pilot program under this section.

(2) Statistical summary data on fellowship awardees disaggregated by race, ethnicity, sex, geography, age, years since completion of doctoral degree, and institution type.

(3) If determined effective, a plan for permanent implementation of the pilot program.

(Pub. L. 117–167, div. B, title VI, §10601, Aug. 9, 2022, 136 Stat. 1632.)

PART B—NATIONAL SCIENCE AND TECHNOLOGY STRATEGY

§ 19221. Strategy and report on the nation's economic security, science, research, and innovation to support the national security strategy

(a) Definitions

In this section:

(1) Foreign country of concern

The term ''foreign country of concern'' means the People's Republic of China, the Democratic People's Republic of Korea, the Russian Federation, the Islamic Republic of Iran, or any other country determined to be a country of concern by the Department of State.

(2) Foreign entity of concern

The term ''foreign entity of concern'' means a foreign entity that is—

(A) designated as a foreign terrorist organization by the Secretary of State under section 1189(a) of title 8;

(B) included on the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury (commonly known as the SDN list);

(C) owned by, controlled by, or subject to the jurisdiction or direction of a government of a foreign country that is a covered nation (as such term is defined in section 4872 of title 10);

(D) alleged by the Attorney General to have been involved in activities for which a conviction was obtained under—

(i) chapter 37 of title 18 (commonly known as the Espionage Act);

(ii) section 951 or 1030 of title 18;

(iii) chapter 90 of title 18 (commonly known as the Economic Espionage Act of 1996);

(iv) the Arms Export Control Act (22 U.S.C. 2751 et seq.);

(v) section 2274, 2275, 2276, 2277, or 2284 of this title;

(vi) the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.); or

(vii) the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.); or

(E) determined by the Secretary of Commerce, in consultation with the Secretary of Defense and the Director of National Intelligence, to be engaged in unauthorized conduct that is detrimental to the national security or foreign policy of the United States.

(3) National security strategy

The term ''national security strategy'' means the national security strategy required under section 3043 of title 50.

(b) Strategy and report

(1) In general

Not later than 90 days after the transmission of each national security strategy under section 3043(a) of title 50, the President, acting through the Director of the Office of Science and Technology Policy, shall, in coordination with the National Science and Technology Council, the National Security Council, the Director of the National Economic Council, and the heads of such other relevant Federal agencies as the Director of the Office of Science and Technology Policy considers appropriate and in consultation with such nongovernmental partners as the Director of the Office of Science and Technology Policy considers appropriate—

(A) review such strategy, including the national defense strategy under subsection (g)

of section 113 of title 10 and the national science and technology strategy under section 6615 of this title, programs, and resources as the Director of the Office of Science and Technology Policy determines pertain to United States' national competitiveness in science, technology, research, innovation, and technology transfer activities, including patenting and licensing, that support the national security strategy;

(B) develop or revise a national strategy to improve the national competitiveness of United States science, technology, research, and innovation to support the national security strategy; and

(C) submit to Congress—

(i) a report on the findings of the Director of the Office of Science and Technology Policy with respect to the review conducted pursuant to subparagraph (A); and

(ii) the strategy developed or revised pursuant to subparagraph (B).

(2) Termination

This subsection terminates on the date that is 5 years after August 9, 2022.

(c) Elements

(1) Report

Each report submitted under subsection (b)(1)(C)(i) shall include the following:

(A) An assessment of the efforts of the United States Government to preserve United States leadership in key emerging technologies and prevent United States strategic competitors from leveraging advanced technologies to gain strategic military or economic advantages over the United States.

(B) An assessment of public and private investment in science and technology relevant to national security purposes, and the implications of such for the geostrategic position of the United States.

(C) A description of the prioritized economic security interests and objectives.

(D) An assessment of global trends in science and technology, including potential threats to the national security of the United States in science and technology.

(E) An assessment of the national debt and its implications for the economic and national security of the United States.

(F) An assessment of how regional innovation capacity efforts in STEM fields are contributing and could contribute to the national security the United States, including programs run by State and local governments.

(G) An assessment of the following:

(i) Workforce needs for competitiveness in technology areas identified in the national security strategy.

(ii) Any efforts needed to expand pathways into technology fields to achieve the goals of the national security strategy.

(H) An assessment of barriers to the development, evolution, or competitiveness of start-ups, small and mid-sized business entities, and industries that are critical to national security.

(I) An assessment of the effectiveness of the Federal Government, federally funded research and development centers, and national laboratories in supporting and promoting the technology commercialization and technology transfer of technologies critical to national security.

(J) An assessment of manufacturing capacity, logistics, and supply chain dynamics of major export sectors that are critical to national security, including access to a skilled workforce, physical infrastructure, and broadband network infrastructure.

(K) An assessment of how the Federal Government is increasing the participation of underrepresented populations in science, research, innovation, and manufacturing.

(L) An assessment of public-private partnerships in technology commercialization in support of national security, including—

(i) the structure of current defense technology research and commercialization arrangements with regard to public-private partnerships; and

(ii) the extent to which intellectual property developed with Federal defense funding—

(I) is being used to manufacture in the United States rather than in other countries; and

(II) is being used by foreign business entities that are majority owned or controlled (as such term is defined in section 800.208 of title 31, Code of Federal Regulations, or a successor regulation), or minority owned greater than 25 percent by—

(aa) any governmental organization of a foreign country of concern; or

(bb) any other entity that is—

(AA) known to be owned or controlled by any governmental organization of a foreign country of concern; or

(BB) organized under, or otherwise subject to, the laws of a foreign country of concern.

(M) Recommendations to enhance the ability of the Federal Government to recruit into Federal service and retain in such service individuals with critical skills relevant to national security.

(N) Recommendations for policies to protect United States leadership and the allies of the United States in critical areas relevant to national security through targeted export controls, investment screening, and counterintelligence activities.

(O) Informed by the interagency process established under section 1758 of the Export Control Reform Act of 2018 [50 U.S.C. 4817], a technology annex, which may be classified, describing an integrated and enduring approach to the identification, prioritization, development, and fielding of emerging technologies relevant to national security.

(2) Strategy

Each strategy submitted under subsection (b)(1)(C)(ii) shall, to the extent practicable, include the following:

(A) A plan to utilize available tools to address or minimize the leading threats and challenges and to take advantage of the leading opportunities, particularly in regards to technologies central to international competition in science and technology relevant to national security purposes, including the following:

(i) Specific objectives, tasks, metrics, and milestones for each relevant Federal agency.

(ii) Strategic objectives and priorities necessary to maintain the leadership of the United States in science and technology relevant to national security purposes, including near-term, medium-term, and long-term research priorities.

(iii) Specific plans to safeguard research and technology funded, as appropriate, in whole or in part, by the Federal Government, including in technologies critical to national security, from theft or exfiltration by foreign entities of concern.

(iv) Specific plans to support public and private sector investment in research, technology development, education and workforce development, and domestic manufacturing supportive of the national security of the United States and to foster the use of public-private partnerships.

(v) A description of the following:

(I) How the strategy submitted under subsection (b)(1)(C)(ii) supports the national security strategy.

(II) How the strategy submitted under such subsection is integrated and coordinated with the most recent—

(aa) national defense strategy under subsection (g) of section 113 of title 10; and

(bb) national science and technology strategy under section 6615 of this title.

(vi) A plan to encourage the governments of countries that are allies or partners of the United States to cooperate with the execution of such strategy, where appropriate.

(vii) A plan for strengthening the industrial base of the United States.

(viii) A plan to remove or update overly burdensome or outdated Federal regulations, as appropriate.

(ix) A plan—

(I) to further incentivize industry participation in public-private partnerships for the purposes of accelerating technology research and commercialization in support of national security, including alternate ways of accounting for in-kind contributions and valuing partially manufactured products;

(II) to ensure that intellectual property developed with Federal funding is commercialized in the United States; and

(III) to ensure, to the maximum appropriate extent, that intellectual property developed with Federal funding is not being used by foreign business entities that are majority owned or controlled (as such term is defined in section 800.208 of title 31, Code of Federal Regulations, or a successor regulation), or minority owned greater than 25 percent by—

(aa) any governmental organization of a foreign country of concern; or

(bb) any other entity that is—

(AA) known to be owned or controlled by any governmental organization of a foreign country of concern; or

(BB) organized under, or otherwise subject to, the laws of a foreign country of concern.

(x) An identification of additional resources, administrative action, or legislative action recommended to assist with the implementation of such strategy.

(d) Research and development funding

The Director of the Office of Science and Technology Policy shall, as the Director of the Office of Science and Technology Policy considers necessary, consult with the Director of the Office of Management and Budget and with the heads of such other elements of the Executive Office of the President as the Director of the Office of Science and Technology Policy considers appropriate to ensure the recommendations and priorities with respect to research and development funding relevant to national security, as expressed in the most recent report and strategy submitted under subsection (b)(1)(C) are incorporated into the development of annual budget requests for Federal research agencies.

(e) Publication

The Director of the Office of Science and Technology Policy shall, consistent with the protection of national security and other sensitive matters and to the maximum extent practicable, make each report submitted under subsection (b)(1)(C)(i) publicly available on an internet website of the Office of Science and Technology Policy. Each such report may include a classified annex if the Director of the Office of Science and Technology Policy determines such is appropriate.

(Pub. L. 117–167, div. B, title VI, §10612, Aug. 9, 2022, 136 Stat. 1635.)

Editorial Notes

REFERENCES IN TEXT

The Arms Export Control Act, referred to in subsec. (a)(2)(D)(iv), is Pub. L. 90–629, Oct. 22, 1968, 82 Stat. 1320, which is classified principally to chapter 39 (§2751 et seq.) of Title 22, Foreign Relations and Intercourse. For complete classification of this Act to the Code, see Short Title note set out under section 2751 of Title 22 and Tables.

The Export Control Reform Act of 2018, referred to in subsec. (a)(2)(D)(vi), is subtitle B (§§1741–1781) of title XVII of div. A of Pub. L. 115–232, Aug. 13, 2018, 132 Stat. 2208, which is classified principally to chapter 58 (§4801 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Short Title note set out under section 4801 of Title 50 and Tables.

The International Emergency Economic Powers Act, referred to in subsec. (a)(2)(D)(vii), is title II of Pub. L. 95–223, Dec. 28, 1977, 91 Stat. 1626, which is classified generally to chapter 35 (§1701 et seq.) of Title 50, War

and National Defense. For complete classification of this Act to the Code, see Short Title note set out under section 1701 of Title 50 and Tables.

§ 19222. National research and development strategy for distributed ledger technology

(a) Definitions

In this section:

(1) Director

Except as otherwise expressly provided, the term ''Director'' means the Director of the Office of Science and Technology Policy.

(2) Distributed ledger

The term ''distributed ledger'' means a ledger that—

(A) is shared across a set of distributed nodes, which are devices or processes, that participate in a network and store a complete or partial replica of the ledger;

(B) is synchronized between the nodes;

(C) has data appended to it by following the ledger's specified consensus mechanism;

(D) may be accessible to anyone (public) or restricted to a subset of participants (private); and

(E) may require participants to have authorization to perform certain actions (engaging) or require no authorization (permissionless).

(3) Distributed ledger technology

The term ''distributed ledger technology'' means technology that enables the operation and use of distributed ledgers.

(4) Institution of higher education

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

(5) Relevant congressional committees

The term ''relevant congressional committees'' means—

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

(B) the Committee on Science, Space, and Technology of the House of Representatives.

(6) Smart contract

The term ''smart contract'' means a computer program stored in a distributed ledger system that is executed when certain predefined conditions are satisfied and wherein the outcome of any execution of the program may be recorded on the distributed ledger.

(b) National distributed ledger technology research and development strategy

(1) In general

The Director, or a designee of the Director, shall, in coordination with the National Science and Technology Council, and the heads of such other relevant Federal agencies and entities as the Director considers appropriate, which may include the National Academies, and in consultation with such nongovernmental entities as the Director considers appropriate, develop a national strategy for the research and development of distributed ledger technologies and their applications, including applications of public and permissionless distributed ledgers. In developing the national strategy, the Director shall consider the following:

(A) Current efforts and coordination by Federal agencies to invest in the research and development of distributed ledger technologies and their applications, including through programs like the Small Business Innovation Research program, the Small Business Technology Transfer program, and the National Science Foundation's Innovation Corps programs.

(B)(i) The potential benefits and risks of applications of distributed ledger technologies across different industry sectors, including their potential to—

(I) lower transactions costs and facilitate new types of commercial transactions;

(II) protect privacy and increase individuals' data sovereignty;

(III) reduce friction to the interoperability of digital systems;

(IV) increase the accessibility, auditability, security, efficiency, and transparency of digital services;

(V) increase market competition in the provision of digital services;

(VI) enable dynamic contracting and contract execution through smart contracts;

(VII) enable participants to collaborate in trustless and disintermediated environments;

(VIII) enable the operations and governance of distributed organizations;

(IX) create new ownership models for digital items; and

(X) increase participation of populations historically underrepresented in the technology, business, and financial sectors.

(ii) In consideration of the potential risks of applications of distributed ledger technologies under clause (i), the Director shall take into account, where applicable—

(I) additional risks that may emerge from distributed ledger technologies, as identified in reports submitted to the President pursuant to Executive Order 14067, that may be addressed by research and development;

(II) software vulnerabilities in distributed ledger technologies and smart contracts;

(III) limited consumer literacy on engaging with applications of distributed ledger technologies in a secure way;

(IV) the use of distributed ledger technologies in illicit finance and their use in combating illicit finance;

(V) manipulative, deceptive, and fraudulent practices that harm consumers engaging with applications of distributed ledger technologies;

(VI) the implications of different consensus mechanisms for digital ledgers and governance and accountability mechanisms for applications of distributed ledger technologies, which may include decentralized networks;