(ii) develop a comprehensive and confidential list, or a bill of materials, of each binary component of the software, firmware, or product that is required to deploy additional secure computing enclaves;

(iii) develop templates for all policies and procedures required to operate the secure computing enclave in a research setting;

(iv) develop a system security plan template; and

(v) develop a process for managing a plan of action and milestones for the secure computing enclave.

(E) Sustainability

In reviewing applications for awards, the Director shall review and consider plans and prospects of the applicant institution of higher education to ensure long-term sustainability of the computing enclave, beyond the availability of Federal funds.

(F) Duration

Subject to other availability of appropriations, the pilot program established pursuant to subparagraph (A) shall operate for not less than 3 years.

(G) Report

(i) In general

The Director shall report to Congress not later than 6 months after the completion of the pilot program under subparagraph (A).

(ii) Contents

The report required under clause (i) shall include—

(I) an assessment of the pilot program under subparagraph (A), including an assessment of the security benefits provided by such secure computing enclaves;

(II) recommendations related to the value of expanding the network of secure computing enclaves; and

(III) recommendations on the efficacy of the use of secure computing enclaves by other Federal agencies in a broader effort to expand security of Federal research.

(H) Authorization of appropriations

There is authorized to be appropriated to the Director, $38,000,000 for fiscal years 2023 through 2025, to carry out the activities outlined in this paragraph.

(Pub. L. 117–167, div. B, title III, §10374, Aug. 9, 2022, 136 Stat. 1571.)

Editorial Notes

CODIFICATION

Section is comprised of section 10374 of Pub. L. 117–167. Subsec. (d)(1) of section 10374 of Pub. L. 117–167 amended section 5511 of Title 15, Commerce and Trade.

§ 19085. National secure data service

(a) In general

The Director, in consultation with the Director of the Office of Management and Budget and the interagency committee established under section 9413 of title 15, shall establish a demonstration project to develop, refine, and test models to inform the full implementation of the Commission on Evidence-Based Policymaking recommendation for a governmentwide data linkage and access infrastructure for statistical activities conducted for statistical purposes, as defined in chapter 35 of title 44.

(b) Establishment

Not later than one year after August 9, 2022, the Director shall establish a National Secure Data Service demonstration project. The National Secure Data Service demonstration project shall be—

(1) aligned with the principles, best practices, and priority actions recommended by the Advisory Committee on Data for Evidence Building, to the extent feasible; and

(2) operated directly by or via a contract that is managed by the National Center for Science and Engineering Statistics.

(c) Data

In carrying out this section, the Director shall engage with Federal and State agencies to collect, acquire, analyze, report, and disseminate statistical data in the United States and other nations to support governmentwide evidence-building activities consistent with the Foundations for Evidence-Based Policymaking Act of 2018.

(d) Voluntary participation

Participation in the National Secure Data Service demonstration project by Federal and State agencies shall be voluntary.

(e) Privacy and confidentiality protections

If the Director issues a management contract under subsection (b), the recipient shall be designated as an ''agent'' under subchapter III of chapter 35 of title 44 with all requirements and obligations for protecting confidential information delineated in the Confidential Information Protection and Statistical Efficiency Act of 2018 and the Privacy Act of 1974.

(f) Technology and privacy standards

In carrying out this subsection, the Director shall—

(1) consider application and use only of systems and technologies that incorporate protection measures to reasonably ensure confidential data and statistical products are protected in accordance with obligations under subchapter III of chapter 35 of title 44, including systems and technologies that ensure—

(A) raw data and other sensitive inputs are not accessible to recipients of statistical outputs from the National Secure Data Service demonstration project;

(B) no individual entity's data or information is revealed by the National Secure Data Service demonstration project platform to any other party in an identifiable form;

(C) no information about the data assets used in the National Secure Data Service demonstration project is revealed to any other party, except as incorporated into the final statistical output;

(D) the National Secure Data Service demonstration project permits only authorized

analysts to perform statistical queries necessary to answer approved project questions, and prohibits any other queries; and

(E) the National Secure Data Service demonstration project conducts privacy risk assessments to minimize the privacy risks to individual entities whose data has been made available by a reporting entity, including those privacy risks that could result from data breaches of any system operated by the reporting entity, as well as for determining approved project questions under subparagraph (D) to minimize the privacy risks to individuals affected by uses of the statistical output; and

(2) the National Secure Data Service demonstration project shall implement reasonable measures commensurate with the risks to individuals' privacy to achieve the outcomes under subparagraphs (A) through (E) of paragraph (1), which may include the appropriate application of privacy-enhancing technologies and appropriate measures to minimize or prevent reidentification risks consistent with any applicable guidance or regulations issued under subchapter III of chapter 35 of title 44.

(g) Transparency

The National Secure Data Service established under subsection (b) shall maintain a public website with up-to-date information on supported projects.

(h) Report

Not later than 2 years after August 9, 2022, the National Secure Data Service demonstration project established under subsection (b) shall submit a report to Congress that includes—

(1) a description of policies for protecting data, consistent with applicable Federal law;

(2) a comprehensive description of all completed or active data linkage activities and projects;

(3) an assessment of the effectiveness of the demonstration project for mitigating risks and removing barriers to a sustained implementation of the National Secure Data Service as recommended by the Commission on Evidence-Based Policymaking; and

(4) if deemed effective by the Director, a plan for scaling up the demonstration project to facilitate data access for evidence building while ensuring transparency and privacy.

(i) Authorization of appropriations

There are authorized to be appropriated to the Director to carry out this subsection $9,000,000 for each of fiscal years 2023 through 2027.

(Pub. L. 117–167, div. B, title III, §10375, Aug. 9, 2022, 136 Stat. 1574.)

Editorial Notes

REFERENCES IN TEXT

The Foundations for Evidence-Based Policymaking Act of 2018, referred to in subsec. (c), is Pub. L. 115–435, Jan. 14, 2019, 132 Stat. 5529. For complete classification of this Act to the Code, see Short Title of 2019 Amendment note set out under section 101 of Title 5, Government Organization and Employees, and Tables.

The Confidential Information Protection and Statistical Efficiency Act of 2018, referred to in subsec. (e), is title III of Pub. L. 115–435, Jan. 14, 2019, 132 Stat. 5544. For complete classification of this Act to the Code, see Short Title of 2019 Amendment note set out under section 101 of Title 44, Public Printing and Documents, and Tables.

The Privacy Act of 1974, referred to in subsec. (e), is Pub. L. 93–579, Dec. 31, 1974, 88 Stat. 1896, which enacted section 552a of Title 5, Government Organization and Employees, and provisions set out as notes under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 Amendment note set out under section 552a of Title 5 and Tables.

PART G—DIRECTORATE FOR TECHNOLOGY, INNOVATION, AND PARTNERSHIPS

§ 19101. Establishment

There is established within the Foundation the Directorate for Technology, Innovation, and Partnerships to advance research and development, technology development, and related solutions to address United States societal, national, and geostrategic challenges, for the benefit of all Americans.

(Pub. L. 117–167, div. B, title III, §10381, Aug. 9, 2022, 136 Stat. 1576.)

§ 19102. Purposes

The purposes of the Directorate established under section 19101 of this title are to—

(1) support use-inspired and translational research and accelerate the development and use of federally funded research;

(2) strengthen United States competitiveness by accelerating the development of key technologies; and

(3) grow the domestic workforce in key technology focus areas, and expand the participation of United States students and researchers in areas of societal, national, and geostrategic importance, at all levels of education.

(Pub. L. 117–167, div. B, title III, §10382, Aug. 9, 2022, 136 Stat. 1576.)

§ 19103. Activities

Subject to the availability of appropriated funds, the Director shall achieve the purposes described in section 19102 of this title by making awards through the Directorate that—

(1) support transformational advances in use-inspired and translational research and technology development, including through diverse funding mechanisms and models at different scales, to include convergence accelerators and projects designed to achieve specific technology metrics or objectives;

(2) encourage the translation of research into innovations, processes, and products, including by—

(A) engaging researchers on topics relevant to United States societal, national, and geostrategic challenges, including by educating researchers on engaging with end users and the public;

(B) advancing novel approaches and reducing barriers to technology transfer, including through intellectual property frameworks between academia and industry, nonprofit entities, venture capital communities, and approaches to technology transfer for applications with public benefit that may