proposal requests that include the purchase, installation, operation, and maintenance of equipment and instrumentation to reduce consumption of helium.

(2) Cost sharing

The Director may waive the cost-sharing requirement for helium conservation measures for non-Ph.D.-granting institutions of higher education and Ph.D.-granting institutions of higher education that are not ranked among the top 100 institutions receiving Federal research and development funding, as documented by the National Center for Science and Engineering Statistics.

(b) Annual report

No later than 1 year after August 9, 2022, and annually for the subsequent two years, the Director shall submit an annual report to Congress on the use of funding awarded by the Foundation for the purchase and conservation of helium. The report should include—

(1) the volume and price of helium purchased;

(2) changes in pricing and availability of helium; and

(3) any supply disruptions impacting a substantial number of institutions.

(Pub. L. 117–167, div. B, title III, § 10373, Aug. 9, 2022, 136 Stat. 1571.)

§ 19084. Advanced computing

(a) Computing needs

To gather information about the computational needs of Foundation-funded projects, the Director shall require award proposals submitted to the Foundation, as appropriate, to include estimates of computational resource needs for projects that require use of advanced computing. The Director shall encourage and provide access to tools that facilitate the inclusion of these measures, including those identified in the 2016 National Academies report entitled ''Future Directions for NSF Advanced Computing Infrastructure to Support U.S. Science and Engineering in 2017–2020''.

(b) Reports

The Director shall document and publish every two years a summary of the amount and types of advanced computing capabilities that are needed to fully meet the Foundation's project needs as identified under subsection (a).

(c) Roadmap

To set priorities and guide strategic decisions regarding investments in advanced computing capabilities, the Director shall develop, publish, and regularly update a 5-year advanced computing roadmap that—

(1) describes the advanced computing resources and capabilities that would fully meet anticipated project needs, including through investments in the Mid-Scale Research Infrastructure program and the Major Research Equipment and Facilities Construction account;

(2) draws on community input, information contained in research proposals, allocation requests, insights from Foundation-funded cyber-infrastructure operators, and Foundation-wide information gathering regarding community needs;

(3) considers computational needs of planned major facilities;

(4) reflects anticipated technology trends;

(5) informs users and potential partners about future facilities and services;

(6) addresses the needs of groups historically underrepresented in STEM and geographic regions with low availability and high demand for advanced computing resources;

(7) considers how Foundation-supported advanced computing capabilities can be leveraged for activities through the Directorate for Technology, Innovation, and Partnerships; and

(8) provides an update to Congress about the level of funding necessary to fully meet computational resource needs for the research community.

(d) Securing American research from cyber theft

(1) Omitted

(2) Computing enclave pilot program

(A) In general

The Director, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Energy, and the heads of other relevant Federal departments and agencies, shall establish a pilot program to make awards to ensure the security of federally supported research data and to assist regional institutions of higher education and their researchers in compliance with regulations regarding the safeguarding of sensitive information and other relevant regulations and Federal guidelines.

(B) Structure

In carrying out the pilot program established pursuant to subparagraph (A), the Director shall select, for the development, installation, maintenance, or sustainment of secure computing enclaves, three institutions of higher education that have an established graduate student program and a demonstrated history of working with secure information, consistent with appropriate security protocols.

(C) Regionalization

(i) In general

In selecting universities pursuant to subparagraph (B), the Director shall give preference to institutions of higher education with the capability of serving other regional universities.

(ii) Geographic dispersal

The enclaves should be geographically dispersed to better meet the needs of regional interests.

(D) Program elements

The Director shall work with institutions of higher education selected pursuant to subparagraph (B) to—

(i) develop an approved design blueprint for compliance with Federal data protection protocols;

(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