(Pub. L. 117–167, div. B, title III, § 10328, Aug. 9, 2022, 136 Stat. 1545.)

§ 19018. Intramural emerging research institutions pilot program

(a) Establishment

The Director may conduct multiple pilot programs, including through existing programs or other programs authorized in this division or division A, within the Foundation to expand the number of institutions of higher education (including such institutions that are community colleges), and other eligible entities that the Director determines appropriate, that are able to successfully compete for Foundation awards.

(b) Components

Pilot programs under this section may include—

(1) a mentorship program;

(2) award application writing technical assistance;

(3) targeted outreach, including to a historically Black college or university, a Tribal college or university, or a minority-serving institution (including a Hispanic-serving institution or an institution of higher education with an established STEM capacity building program focused on Native Hawaiians or Alaska Natives);

(4) programmatic support or solutions for institutions or entities that do not have an experienced award management office;

(5) an increase in the number of award proposal reviewers from institutions of higher education that have not traditionally received funds from the Foundation; or

(6) an increase of the term and funding, for a period of 3 years or less, as appropriate, for awards with a first-time principal investigator, when paired with regular mentoring on the administrative aspects of award management.

(c) Limitation

As appropriate, each pilot program under this section shall work to reduce administrative burdens for recipients and award personnel.

(d) Agency-wide programs

Not later than 5 years after August 9, 2022, the Director shall—

(1) review the results of the pilot programs under this section; and

(2) develop agencywide best practices from the pilot programs for implementation across the Foundation, in order to fulfill the requirement under section 1862(e) of this title.

(Pub. L. 117–167, div. B, title III, § 10330, Aug. 9, 2022, 136 Stat. 1550.)

Editorial Notes

REFERENCES IN TEXT

This division, referred to in subsec. (a), is div. B of Pub. L. 117–167, Aug. 9, 2022, 136 Stat. 1399, which enacted this chapter and enacted, amended, and repealed numerous other sections and notes in the Code. For complete classification of div. B to the Code, see Short Title note set out under section 18901 of this title and Tables.

Division A, referred to in subsec. (a), is div. A of Pub. L. 117–167, Aug. 9, 2022, 136 Stat. 1372, known as the CHIPS Act of 2022. For complete classification of div. A to the Code, see Short Title of 2022 Amendment note set out under section 4651 of Title 15, Commerce and Trade, and Tables.

PART D—NSF RESEARCH SECURITY

§ 19031. Office of Research Security and Policy

The Director shall maintain a Research Security and Policy office within the Office of the Director with not fewer than four full-time equivalent positions, in addition to the Chief of Research Security established pursuant to section 19032 of this title. The functions of the Research Security and Policy office shall be to coordinate all research security policy issues across the Foundation, including by—

(1) consulting and coordinating with the Foundation Office of Inspector General, with other Federal research agencies, and intelligence and law enforcement agencies, and the National Science and Technology Council, as appropriate, in accordance with the authority provided under section 1746 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 42 U.S.C. 6601 note), to identify and address potential security risks that threaten research integrity and other risks to the research enterprise and to develop research security policy and best practices, taking into account the policy guidelines to be issued by the Director of the Office of Science and Technology Policy under section 19231 of this title;

(2) serving as a resource at the Foundation for all issues related to the security and integrity of the conduct of Foundation-supported research;

(3) conducting outreach and education activities for recipients on research policies and potential security risks and on policies and activities to protect intellectual property and information about critical technologies relevant to national security, consistent with the controls relevant to the grant or award;

(4) educating Foundation program managers and other directorate staff on evaluating Foundation awards and recipients for potential security risks;

(5) communicating reporting and disclosure requirements to recipients and applicants for funding;

(6) performing risk assessments, in consultation, as appropriate, with other Federal agencies, of Foundation proposals and awards using analytical tools to assess nondisclosures of required information;

(7) establishing policies and procedures for identifying, communicating, and addressing security risks that threaten the integrity of Foundation-supported research and development, working in consultation, as appropriate, with other Federal agencies, to ensure compliance with National Security Presidential Memorandum–33 (relating to strengthening protections of United States Government-supported research and development against foreign government interference and exploitation) or a successor policy document; and

(8) in accordance with relevant policies of the agency, conducting or facilitating due dili-