

2(b) of div. W of Pub. L. 117-103, which is set out as a note under section 12291 of this title.

§ 30108. National Resource Center grant

(a) Definitions

In this section:

(1) Cybercrime against individuals

The term “cybercrime against individuals” has the meaning given such term in section 30107 of this title.

(2) Eligible entity

The term “eligible entity” means a non-profit private organization that—

(A) focuses on cybercrimes against individuals;

(B) provides documentation to the Attorney General demonstrating experience working directly on issues of cybercrimes against individuals; and

(C) includes on the organization’s advisory board representatives who—

(i) have a documented history of working directly on issues of cybercrimes against individuals;

(ii) have a history of working directly with victims of cybercrimes against individuals; and

(iii) are geographically and culturally diverse.

(b) Authorization of grant program

Subject to the availability of appropriations, the Attorney General shall award a grant under this section to an eligible entity for the purpose of the establishment and maintenance of a National Resource Center on Cybercrimes Against Individuals to provide resource information, training, and technical assistance to improve the capacity of individuals, organizations, governmental entities, and communities to prevent, enforce, and prosecute cybercrimes against individuals.

(c) Application

(1) In general

To request a grant under this section, an eligible entity shall submit an application to the Attorney General not later than 90 days after the date on which funds to carry out this section are appropriated for fiscal year 2022 in such form as the Attorney General may require.

(2) Contents

An application submitted under paragraph (1) shall include the following:

(A) An assurance that, for each fiscal year covered by the application, the applicant will maintain and report such data, records, and information (programmatic and financial) as the Attorney General may reasonably require.

(B) A certification, made in a form acceptable to the Attorney General, that—

(i) the programs funded by the grant meet all the requirements of this section;

(ii) all the information contained in the application is correct; and

(iii) the applicant will comply with all provisions of this section and all other applicable Federal laws.

(d) Use of funds

The eligible entity awarded a grant under this section shall use such amounts for the establishment and maintenance of a National Resource Center on Cybercrimes Against Individuals, which shall—

(1) offer a comprehensive array of technical assistance and training resources to Federal, State, and local governmental agencies, community-based organizations, and other professionals and interested parties related to cybercrimes against individuals, including programs and research related to victims;

(2) maintain a resource library which shall collect, prepare, analyze, and disseminate information and statistics related to—

(A) the incidence of cybercrimes against individuals;

(B) the enforcement and prosecution of laws relating to cybercrimes against individuals; and

(C) the provision of supportive services and resources for victims, including victims from underserved populations, of cybercrimes against individuals; and

(3) conduct research related to—

(A) the causes of cybercrimes against individuals;

(B) the effect of cybercrimes against individuals on victims of such crimes; and

(C) model solutions to prevent or deter cybercrimes against individuals or to enforce the laws relating to cybercrimes against individuals.

(e) Duration of grant

(1) In general

A grant awarded under this section shall be awarded for a period of 5 years.

(2) Renewal

A grant under this section may be renewed for additional 5-year periods if the Attorney General determines that the funds made available to the recipient were used in a manner described in subsection (d), and if the recipient resubmits an application described in subsection (c) in such form, and at such time, as the Attorney General may reasonably require.

(f) Subgrants

The eligible entity awarded a grant under this section may make subgrants to other nonprofit private organizations with relevant subject matter expertise in order to establish and maintain the National Resource Center on Cybercrimes Against Individuals in accordance with subsection (d).

(g) Reports to the Attorney General

On the date that is 1 year after the date on which an eligible entity receives a grant under this section, and annually thereafter for the duration of the grant period, the entity shall submit to the Attorney General a report which contains—

(1) a summary of the activities carried out under the grant program during the previous year;

(2) an evaluation of the results of such activities; and

(3) such other information as the Attorney General may reasonably require.

(h) Reports to Congress

Not later than November 1 of each even-numbered fiscal year, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report that contains a compilation of the information contained in the reports submitted under subsection (g).

(i) Authorization of appropriations

There are authorized to be appropriated to carry out this section \$4,000,000 for each of fiscal years 2023 through 2027.

(Pub. L. 117–103, div. W, title XIV, §1402, Mar. 15, 2022, 136 Stat. 948.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section not effective until Oct. 1 of the first fiscal year beginning after Mar. 15, 2022, see section 4(a) of div. W of Pub. L. 117–103, set out as a note under section 6851 of Title 15, Commerce and Trade.

DEFINITIONS

For definitions of terms used in this section, see section 12291 of this title, as made applicable by section 2(b) of div. W of Pub. L. 117–103, which is set out as a note under section 12291 of this title.

§ 30109. National strategy, classification, and reporting on cybercrime

(a) Definitions

In this section:

(1) Computer

The term “computer” includes a computer network and any interactive electronic device.

(2) Cybercrime against individuals

The term “cybercrime against individuals” has the meaning given the term in section 30107 of this title.

(b) National strategy

The Attorney General shall develop a national strategy to—

(1) reduce the incidence of cybercrimes against individuals;

(2) coordinate investigations of cybercrimes against individuals by Federal law enforcement agencies;

(3) increase the number of Federal prosecutions of cybercrimes against individuals; and

(4) develop an evaluation process that measures rates of cybercrime victimization and prosecutorial rates among Tribal and culturally specific communities.

(c) Classification of cybercrimes against individuals for purposes of crime reports

In accordance with the authority of the Attorney General under section 534 of title 28, the Director of the Federal Bureau of Investigation shall—

(1) design and create within the Uniform Crime Reports a category for offenses that constitute cybercrimes against individuals;

(2) to the extent feasible, within the category established under paragraph (1), estab-

lish subcategories for each type of cybercrime against individuals that is an offense under Federal or State law;

(3) classify the category established under paragraph (1) as a Part I crime in the Uniform Crime Reports; and

(4) classify each type of cybercrime against individuals that is an offense under Federal or State law as a Group A offense for the purpose of the National Incident-Based Reporting System.

(d) Annual summary

The Attorney General shall publish an annual summary of the information reported in the Uniform Crime Reports and the National Incident-Based Reporting System relating to cybercrimes against individuals, including an evaluation of the implementation process for the national strategy developed under subsection (b) and outcome measurements on its impact on Tribal and culturally specific communities.

(Pub. L. 117–103, div. W, title XIV, §1403, Mar. 15, 2022, 136 Stat. 950.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section not effective until Oct. 1 of the first fiscal year beginning after Mar. 15, 2022, see section 4(a) of div. W of Pub. L. 117–103, set out as a note under section 6851 of Title 15, Commerce and Trade.

NATIONAL STRATEGY, CLASSIFICATION, AND REPORTING ON CYBERCRIME

(Pub. L. 117–347, title III, §311(a), Jan. 5, 2023, 136 Stat. 6205, provided that:

“(a) NATIONAL STRATEGY.—The Attorney General, in consultation with the Secretary of Homeland Security, shall develop a national strategy, which shall be developed to supplement, not duplicate, the National Strategy to Combat Human Trafficking and the National Strategy for Child Exploitation Prevention and Interdiction of the Department of Justice, to—

“(1) reduce the incidence of cybercrimes against individuals;

“(2) coordinate investigations of cybercrimes against individuals by Federal law enforcement agencies; and

“(3) increase the number of Federal prosecutions of cybercrimes against individuals.”

[For definition of “cybercrime against individuals” as used in section 311(a) of Pub. L. 117–347, set out above, see section 30107(a) of this title, as made applicable by section 3 of Pub. L. 117–347, which is set out as a note under section 20145 of this title.]

BETTER CYBERCRIME METRICS

(Pub. L. 117–116, May 5, 2022, 136 Stat. 1180, as amended by Pub. L. 117–347, title III, §311(b), Jan. 5, 2023, 136 Stat. 6205, provided that:

“SECTION 1. SHORT TITLE.

“This Act may be cited as the ‘Better Cybercrime Metrics Act’.

“SEC. 2. FINDINGS.

“Congress finds the following:

“(1) Public polling indicates that cybercrime could be the most common crime in the United States.

“(2) The United States lacks comprehensive cybercrime data and monitoring, leaving the country less prepared to combat cybercrime that threatens national and economic security.

“(3) In addition to existing cybercrime vulnerabilities, the people of the United States and