§ 30107. Local law enforcement grants for enforcement of cybercrimes

(a) Definitions

In this section:

(1) Computer

The term ''computer'' includes a computer network and an interactive electronic device.

(2) Cybercrime against individuals

The term ''cybercrime against individuals''—

(A) means a criminal offense applicable in the area under the jurisdiction of the relevant State, Indian Tribe, or unit of local government that involves the use of a computer to harass, threaten, stalk, extort, coerce, cause fear to, or intimidate an individual, or without consent distribute intimate images of an adult, except that use of a computer need not be an element of such an offense; and

(B) does not include the use of a computer to cause harm to a commercial entity, government agency, or non-natural person.

(3) Indian tribe; State; Tribal government; unit of local government

The terms ''Indian Tribe'', ''State'', ''Tribal government'', and ''unit of local government'' have the meanings given such terms in section 12291(a) of this title, as amended by this Act.

(b) Authorization of grant program

Subject to the availability of appropriations, the Attorney General shall award grants under this section to States, Indian Tribes, and units of local government for the prevention, enforcement, and prosecution of cybercrimes against individuals.

(c) Application

(1) In general

To request a grant under this section, the chief executive officer of a State, Tribal government, or unit of local government 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 a fiscal year, in such form as the Attorney General may require.

(2) Contents

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

(A) A certification that Federal funds made available under this section will not be used to supplant State, Tribal, or local funds, but will be used to increase the amounts of such funds that would, in the absence of Federal funds, be made available for law enforcement activities.

(B) An assurance that, not later than 30 days before the application (or any amendment to the application) was submitted to the Attorney General, the application (or amendment) was submitted for review to the governing body of the State, Tribe, or unit of local government (or to an organization designated by that governing body).

(C) An assurance that, before the application (or any amendment to the application) was submitted to the Attorney General—

(i) the application (or amendment) was made public; and

(ii) an opportunity to comment on the application (or amendment) was provided to citizens, to neighborhood or community-based organizations, and to victim service providers, to the extent applicable law or established procedure makes such an opportunity available;

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

(E) A certification, made in a form acceptable to the Attorney General and executed by the chief executive officer of the applicant (or by another officer of the applicant, if qualified under regulations promulgated by the Attorney General), that—

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

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

(iii) there has been appropriate coordination with affected agencies; and

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

(F) A certification that the State, Tribe, or in the case of a unit of local government, the State in which the unit of local government is located, has in effect criminal laws which prohibit cybercrimes against individuals.

(G) A certification that any equipment described in subsection (d)(8) purchased using grant funds awarded under this section will be used primarily for investigations and forensic analysis of evidence in matters involving cybercrimes against individuals.

(d) Use of funds

Grants awarded under this section may be used only for programs that provide—

(1) training for State, Tribal, or local law enforcement personnel relating to cybercrimes against individuals, including—

(A) training such personnel to identify and protect victims of cybercrimes against individuals, provided that the training is developed in collaboration with victim service providers;

(B) training such personnel to utilize Federal, State, Tribal, local, and other resources to assist victims of cybercrimes against individuals;

(C) training such personnel to identify and investigate cybercrimes against individuals;

(D) training such personnel to enforce and utilize the laws that prohibit cybercrimes against individuals;

(E) training such personnel to utilize technology to assist in the investigation of cybercrimes against individuals and enforcement of laws that prohibit such crimes; and

(F) the payment of overtime incurred as a result of such training;

(2) training for State, Tribal, or local prosecutors, judges, and judicial personnel relating to cybercrimes against individuals, including—

(A) training such personnel to identify, investigate, prosecute, or adjudicate cybercrimes against individuals;

(B) training such personnel to utilize laws that prohibit cybercrimes against individuals;

(C) training such personnel to utilize Federal, State, Tribal, local, and other resources to assist victims of cybercrimes against individuals; and

(D) training such personnel to utilize technology to assist in the prosecution or adjudication of acts of cybercrimes against individuals, including the use of technology to protect victims of such crimes;

(3) training for State, Tribal, or local emergency dispatch personnel relating to cybercrimes against individuals, including—

(A) training such personnel to identify and protect victims of cybercrimes against individuals;

(B) training such personnel to utilize Federal, State, Tribal, local, and other resources to assist victims of cybercrimes against individuals;

(C) training such personnel to utilize technology to assist in the identification of and response to cybercrimes against individuals; and

(D) the payment of overtime incurred as a result of such training;

(4) assistance to State, Tribal, or local law enforcement agencies in enforcing laws that prohibit cybercrimes against individuals, including expenses incurred in performing enforcement operations, such as overtime payments;

(5) assistance to State, Tribal, or local law enforcement agencies in educating the public in order to prevent, deter, and identify violations of laws that prohibit cybercrimes against individuals;

(6) assistance to State, Tribal, or local law enforcement agencies to support the placement of victim assistants to serve as liaisons between victims of cybercrimes against individuals and personnel of law enforcement agencies;

(7) assistance to State, Tribal, or local law enforcement agencies to establish task forces that operate solely to conduct investigations, forensic analyses of evidence, and prosecutions in matters involving cybercrimes against individuals;

(8) assistance to State, Tribal, or local law enforcement agencies and prosecutors in acquiring computers, computer equipment, and other equipment necessary to conduct investigations and forensic analysis of evidence in matters involving cybercrimes against individuals, including expenses incurred in the training, maintenance, or acquisition of technical updates necessary for the use of such equipment for the duration of a reasonable period of use of such equipment;

(9) assistance in the facilitation and promotion of sharing, with State, Tribal, and local law enforcement agencies and prosecutors, of the expertise and information of Federal law enforcement agencies about the investigation, analysis, and prosecution of matters involving laws that prohibit cybercrimes against individuals, including the use of multijurisdictional task forces; or

(10) assistance to State, Tribal, and local law enforcement and prosecutors in processing interstate extradition requests for violations of laws involving cybercrimes against individuals, including expenses incurred in the extradition of an offender from one State to another.

(e) Reports to the Attorney General

On the date that is 1 year after the date on which a State, Indian Tribe, or unit of local government receives a grant under this section, and annually thereafter, the chief executive officer of the State, Tribal government, or unit of local government shall submit to the Attorney General a report which contains—

(1) a summary of the activities carried out during the previous year with any grant received under this section by such State, Indian Tribe, or unit of local government;

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

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

(f) 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 (e).

(g) Authorization of appropriations

(1) In general

There are authorized to be appropriated to carry out this section $10,000,000 for each of fiscal years 2023 through 2027.

(2) Limitation

Of the amount made available under paragraph (1) in any fiscal year, not more than 5 percent may be used for evaluation, monitoring, technical assistance, salaries, and administrative expenses.

(Pub. L. 117–103, div. W, title XIV, § 1401, Mar. 15, 2022, 136 Stat. 945.)

Editorial Notes

REFERENCES IN TEXT

This Act, referred to in subsec. (a)(3), means div. W of Pub. L. 117–103, section 2(a)(1) of which amended section 12291(a) of this title.

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.

§ 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 nonprofit 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