(2) informational materials, including brochures, videos, posters, and websites to support and supplement the training and educational programs described in paragraph (1).

(Pub. L. 106–468, title II, § 206, as added Pub. L. 115–401, § 2(5), Dec. 31, 2018, 132 Stat. 5341.)

§ 21907. Authorization of appropriations

There is authorized to be appropriated to the Attorney General $3,000,000 to carry out the Ashanti Alert communications network as authorized under this chapter for each of fiscal years 2019 through 2022.

(Pub. L. 106–468, title II, § 207, as added Pub. L. 115–401, § 2(5), Dec. 31, 2018, 132 Stat. 5341.)

Subtitle III—Prevention of Particular Crimes

CHAPTER 301—COMPUTER CRIMES AND INTELLECTUAL PROPERTY CRIMES

Sec.

§ 30101. State grant program for training and prosecution of computer crimes

(a) In general

Subject to the availability of amounts provided in advance in appropriations Acts, the Office of Justice Programs shall make a grant to each State, which shall be used by the State, in conjunction with units of local government, State and local courts, other States, or combinations thereof in accordance with subsection (b).

(b) Use of grant amounts

Grants under this section may be used to establish and develop programs to—

(1) assist State and local law enforcement agencies in enforcing State and local criminal laws relating to computer crime, including infringement of copyrighted works over the Internet;

(2) assist State and local law enforcement agencies in educating the public to prevent and identify computer crime, including infringement of copyrighted works over the Internet;

(3) educate and train State and local law enforcement officers and prosecutors to conduct investigations and forensic analyses of evidence and prosecutions of computer crime, including infringement of copyrighted works over the Internet;

(4) assist State and local law enforcement officers and prosecutors in acquiring computer and other equipment to conduct investigations and forensic analysis of evidence of computer crimes; and

(5) facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer crimes with State and local law enforcement officers and prosecutors, including the use of multijurisdictional task forces.

(c) Assurances

To be eligible to receive a grant under this section, a State shall provide assurances to the Attorney General that the State—

(1) has in effect laws that penalize computer crime, such as criminal laws prohibiting—

(A) fraudulent schemes executed by means of a computer system or network;

(B) the unlawful damaging, destroying, altering, deleting, removing of computer software, or data contained in a computer, computer system, computer program, or computer network; or

(C) the unlawful interference with the operation of or denial of access to a computer, computer program, computer system, or computer network;

(2) an assessment of the State and local resource needs, including criminal justice resources being devoted to the investigation and enforcement of computer crime laws; and

(3) a plan for coordinating the programs funded under this section with other federally funded technical assistant and training programs, including directly funded local programs such as the Local Law Enforcement Block Grant program (described under the heading ''Violent Crime Reduction Programs, State and Local Law Enforcement Assistance'' of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1998 (Public Law 105–119)).

(d) Matching funds

The Federal share of a grant received under this section may not exceed 90 percent of the costs of a program or proposal funded under this section unless the Attorney General waives, wholly or in part, the requirements of this subsection.

(e) Authorization of appropriations

(1) In general

There is authorized to be appropriated to carry out this section $25,000,000 for each of fiscal years 2009 through 2013.

(2) Limitations

Of the amount made available to carry out this section in any fiscal year not more than 3 percent may be used by the Attorney General for salaries and administrative expenses.

(3) Minimum amount

Unless all eligible applications submitted by any State or unit of local government within

such State for a grant under this section have been funded, such State, together with grantees within the State (other than Indian tribes), shall be allocated in each fiscal year under this section not less than 0.75 percent of the total amount appropriated in the fiscal year for grants pursuant to this section, except that the United States Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands each shall be allocated 0.25 percent.

(f) Grants to Indian tribes

Notwithstanding any other provision of this section, the Attorney General may use amounts made available under this section to make grants to Indian tribes for use in accordance with this section.

(Pub. L. 106–572, § 2, Dec. 28, 2000, 114 Stat. 3058; Pub. L. 110–403, title IV, § 401(a), Oct. 13, 2008, 122 Stat. 4271.)

Editorial Notes

REFERENCES IN TEXT

The Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1998, referred to in subsec. (c)(3), is Pub. L. 105–119, Nov. 26, 1997, 111 Stat. 2440. Provisions under the heading ''Violent Crime Reduction Programs, State and Local Law Enforcement Assistance'', 111 Stat. 2452, are not classified to the Code.

CODIFICATION

Section was formerly classified to section 3713 of Title 42, The Public Health and Welfare, prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2008—Subsec. (b)(1)–(3). Pub. L. 110–403, § 401(a)(1), inserted '', including infringement of copyrighted works over the Internet'' after ''computer crime''.

Subsec. (e)(1). Pub. L. 110–403, § 401(a)(2), substituted ''2009 through 2013'' for ''2001 through 2004''.

Statutory Notes and Related Subsidiaries

SHORT TITLE

For short title of Pub. L. 106–572, which is classified to this section, as the ''Computer Crime Enforcement Act'', see section 1 of Pub. L. 106–572, set out as a Short Title of 2000 Act note under section 10101 of this title.

§ 30102. Development and support of cybersecurity forensic capabilities

(a) In general

The Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability—

(1) to provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyberterrorism);

(2) to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime (including cyberterrorism);

(3) to assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime;

(4) to facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces; and

(5) to carry out such other activities as the Attorney General considers appropriate.

(b) Authorization of appropriations

(1) Authorization

There is hereby authorized to be appropriated in each fiscal year $50,000,000 for purposes of carrying out this section.

(2) Availability

Amounts appropriated pursuant to the authorization of appropriations in paragraph (1) shall remain available until expended.

(Pub. L. 107–56, title VIII, § 816, Oct. 26, 2001, 115 Stat. 385.)

Editorial Notes

CODIFICATION

Section was formerly classified as a note under section 509 of Title 28, Judiciary and Judicial Procedure, prior to editorial reclassification and renumbering as this section.

§ 30103. Local law enforcement grants

(a) Omitted

(b) Grants

The Office of Justice Programs of the Department of Justice may make grants to eligible State or local law enforcement entities, including law enforcement agencies of municipal governments and public educational institutions, for training, prevention, enforcement, and prosecution of intellectual property theft and infringement crimes (in this subsection referred to as ''IP–TIC grants''), in accordance with the following:

(1) Use of IP–TIC grant amounts

IP–TIC grants may be used to establish and develop programs to do the following with respect to the enforcement of State and local true name and address laws and State and local criminal laws on anti-infringement, anticounterfeiting, and unlawful acts with respect to goods by reason of their protection by a patent, trademark, service mark, trade secret, or other intellectual property right under State or Federal law:

(A) Assist State and local law enforcement agencies in enforcing those laws, including by reimbursing State and local entities for expenses incurred in performing enforcement operations, such as overtime payments and storage fees for seized evidence.

(B) Assist State and local law enforcement agencies in educating the public to prevent, deter, and identify violations of those laws.

(C) Educate and train State and local law enforcement officers and prosecutors to con-

duct investigations and forensic analyses of evidence and prosecutions in matters involving those laws.

(D) Establish task forces that include personnel from State or local law enforcement entities, or both, exclusively to conduct investigations and forensic analyses of evidence and prosecutions in matters involving those laws.

(E) Assist State and local law enforcement officers and prosecutors in acquiring computer and other equipment to conduct investigations and forensic analyses of evidence in matters involving those laws.

(F) Facilitate and promote the sharing, with State and local law enforcement officers and prosecutors, of the expertise and information of Federal law enforcement agencies about the investigation, analysis, and prosecution of matters involving those laws and criminal infringement of copyrighted works, including the use of multijurisdictional task forces.

(2) Eligibility

To be eligible to receive an IP–TIC grant, a State or local government entity shall provide to the Attorney General, in addition to the information regularly required to be provided under the Financial Guide issued by the Office of Justice Programs and any other information required of Department of Justice's grantees—

(A) assurances that the State in which the government entity is located has in effect laws described in paragraph (1);

(B) an assessment of the resource needs of the State or local government entity applying for the grant, including information on the need for reimbursements of base salaries and overtime costs, storage fees, and other expenditures to improve the investigation, prevention, or enforcement of laws described in paragraph (1); and

(C) a plan for coordinating the programs funded under this section with other federally funded technical assistance and training programs, including directly funded local programs such as the Edward Byrne Memorial Justice Assistance Grant Program authorized by subpart 1 of part E of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3750 et seq.).[1]

(3) Matching funds

The Federal share of an IP–TIC grant may not exceed 50 percent of the costs of the program or proposal funded by the IP–TIC grant.

(4) Authorization of appropriations

(A) Authorization

There is authorized to be appropriated to carry out this subsection the sum of $25,000,000 for each of fiscal years 2009 through 2013.

(B) Limitation

Of the amount made available to carry out this subsection in any fiscal year, not more than 3 percent may be used by the Attorney General for salaries and administrative expenses.

(Pub. L. 110–403, title IV, § 401, Oct. 13, 2008, 122 Stat. 4271.)

Editorial Notes

REFERENCES IN TEXT

The Omnibus Crime Control and Safe Streets Act of 1968, referred to in subsec. (b)(2)(C), is Pub. L. 90–351, June 19, 1968, 82 Stat. 197. Subpart 1 of part E of title I of the Act was classified generally to part A (§ 3750 et seq.) of subchapter V of chapter 46 of Title 42, The Public Health and Welfare, prior to editorial reclassification as part A (§ 10151 et seq.) of chapter 101 of this title. For complete classification of this Act to the Code, see Short Title of 1968 Act note set out under section 10101 of this title and Tables.

CODIFICATION

Section is comprised of section 401 of Pub. L. 110–403. Subsec. (a) of section 401 of Pub. L. 110–403 amended section 30101 of this title.

Section was formerly classified to section 3713a of Title 42, The Public Health and Welfare, prior to editorial reclassification and renumbering as this section.

§ 30104. Improved investigative and forensic resources for enforcement of laws related to intellectual property crimes

(a) In general

Subject to the availability of appropriations to carry out this subsection, the Attorney General, in consultation with the Director of the Federal Bureau of Investigation, shall, with respect to crimes related to the theft of intellectual property—

(1) ensure that there are at least 10 additional operational agents of the Federal Bureau of Investigation designated to support the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice in the investigation and coordination of intellectual property crimes;

(2) ensure that any Computer Hacking and Intellectual Property Crime Unit in the Department of Justice is supported by at least 1 agent of the Federal Bureau of Investigation (in addition to any agent supporting such unit as of October 13, 2008) to support such unit for the purpose of investigating or prosecuting intellectual property crimes;

(3) ensure that all Computer Hacking and Intellectual Property Crime Units located at an office of a United States Attorney are assigned at least 2 Assistant United States Attorneys responsible for investigating and prosecuting computer hacking or intellectual property crimes; and

(4) ensure the implementation of a regular and comprehensive training program—

(A) the purpose of which is to train agents of the Federal Bureau of Investigation in the investigation and prosecution of such crimes and the enforcement of laws related to intellectual property crimes; and

(B) that includes relevant forensic training related to investigating and prosecuting intellectual property crimes.

(b) Organized crime plan

Subject to the availability of appropriations to carry out this subsection, and not later than

[1] See References in Text note below.

180 days after October 13, 2008, the Attorney General, through the United States Attorneys' Offices, the Computer Crime and Intellectual Property section, and the Organized Crime and Racketeering section of the Department of Justice, and in consultation with the Federal Bureau of Investigation and other Federal law enforcement agencies, such as the Department of Homeland Security, shall create and implement a comprehensive, long-range plan to investigate and prosecute international organized crime syndicates engaging in or supporting crimes relating to the theft of intellectual property.

(c) Authorization

There are authorized to be appropriated to carry out this section $10,000,000 for each of fiscal years 2009 through 2013.

(Pub. L. 110–403, title IV, § 402, Oct. 13, 2008, 122 Stat. 4272.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 3713b of Title 42, The Public Health and Welfare, prior to editorial reclassification and renumbering as this section.

§ 30105. Additional funding for resources to investigate and prosecute intellectual property crimes and other criminal activity involving computers

(a) Additional funding for resources

(1) Authorization

In addition to amounts otherwise authorized for resources to investigate and prosecute intellectual property crimes and other criminal activity involving computers, there are authorized to be appropriated for each of the fiscal years 2009 through 2013—

(A) $10,000,000 to the Director of the Federal Bureau of Investigation; and

(B) $10,000,000 to the Attorney General for the Criminal Division of the Department of Justice.

(2) Availability

Any amounts appropriated under paragraph (1) shall remain available until expended.

(b) Use of additional funding

Funds made available under subsection (a) shall be used by the Director of the Federal Bureau of Investigation and the Attorney General, for the Federal Bureau of Investigation and the Criminal Division of the Department of Justice, respectively, to—

(1) hire and train law enforcement officers to—

(A) investigate intellectual property crimes and other crimes committed through the use of computers and other information technology, including through the use of the Internet; and

(B) assist in the prosecution of such crimes; and

(2) enable relevant units of the Department of Justice, including units responsible for investigating computer hacking or intellectual property crimes, to procure advanced tools of forensic science and expert computer forensic assistance, including from non-governmental entities, to investigate, prosecute, and study such crimes.

(Pub. L. 110–403, title IV, § 403, Oct. 13, 2008, 122 Stat. 4273.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 3713c of Title 42, The Public Health and Welfare, prior to editorial reclassification and renumbering as this section.

§ 30106. Annual reports

(a) Report of the Attorney General

Not later than 1 year after October 13, 2008, and annually thereafter, the Attorney General shall submit a report to Congress on actions taken to carry out sections 30103 to 30106 of this title. The initial report required under this subsection shall be submitted by May 1, 2009. All subsequent annual reports shall be submitted by May 1st of each fiscal year thereafter. The report required under this subsection may be submitted as part of the annual performance report of the Department of Justice, and shall include the following:

(1) With respect to grants issued under section 30103 of this title, the number and identity of State and local law enforcement grant applicants, the number of grants issued, the dollar value of each grant, including a break down of such value showing how the recipient used the funds, the specific purpose of each grant, and the reports from recipients of the grants on the efficacy of the program supported by the grant. The Department of Justice shall use the information provided by the grant recipients to produce a statement for each individual grant. Such statement shall state whether each grantee has accomplished the purposes of the grant as established in section 30103(b) of this title. Those grantees not in compliance with the requirements of sections 30103 to 30106 of this title shall be subject, but not limited to, sanctions as described in the Financial Guide issued by the Office of Justice Programs at the Department of Justice.

(2) With respect to the additional agents of the Federal Bureau of Investigation authorized under paragraphs (1) and (2) of section 30104(a) of this title, the number of investigations and actions in which such agents were engaged, the type of each action, the resolution of each action, and any penalties imposed in each action.

(3) With respect to the training program authorized under section 30104(a)(4) of this title, the number of agents of the Federal Bureau of Investigation participating in such program, the elements of the training program, and the subject matters covered by the program.

(4) With respect to the organized crime plan authorized under section 30104(b) of this title, the number of organized crime investigations and prosecutions resulting from such plan.

(5) With respect to the authorizations under section 30105 of this title—

(A) the number of law enforcement officers hired and the number trained;

(B) the number and type of investigations and prosecutions resulting from the hiring and training of such law enforcement officers;

(C) the defendants involved in any such prosecutions;

(D) any penalties imposed in each such successful prosecution;

(E) the advanced tools of forensic science procured to investigate, prosecute, and study computer hacking or intellectual property crimes; and

(F) the number and type of investigations and prosecutions in such tools were used.

(6) Any other information that the Attorney General may consider relevant to inform Congress on the effective use of the resources authorized under sections 30103, 30104, and 30105 of this title.

(7) A summary of the efforts, activities, and resources the Department of Justice has allocated to the enforcement, investigation, and prosecution of intellectual property crimes, including—

(A) a review of the policies and efforts of the Department of Justice related to the prevention and investigation of intellectual property crimes, including efforts at the Office of Justice Programs, the Criminal Division of the Department of Justice, the Executive Office of United States Attorneys, the Office of the Attorney General, the Office of the Deputy Attorney General, the Office of Legal Policy, and any other agency or bureau of the Department of Justice whose activities relate to intellectual property;

(B) a summary of the overall successes and failures of such policies and efforts;

(C) a review of the investigative and prosecution activity of the Department of Justice with respect to intellectual property crimes, including—

(i) the number of investigations initiated related to such crimes;

(ii) the number of arrests related to such crimes; and

(iii) the number of prosecutions for such crimes, including—

(I) the number of defendants involved in such prosecutions;

(II) whether the prosecution resulted in a conviction; and

(III) the sentence and the statutory maximum for such crime, as well as the average sentence imposed for such crime; and

(D) a Department-wide assessment of the staff, financial resources, and other resources (such as time, technology, and training) devoted to the enforcement, investigation, and prosecution of intellectual property crimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting intellectual property crimes.

(8) A summary of the efforts, activities, and resources that the Department of Justice has taken to—

(A) minimize duplicating the efforts, materials, facilities, and procedures of any other Federal agency responsible for the enforcement, investigation, or prosecution of intellectual property crimes; and

(B) enhance the efficiency and consistency with which Federal funds and resources are expended to enforce, investigate, or prosecute intellectual property crimes, including the extent to which the Department has utilized existing personnel, materials, technologies, and facilities.

(b) Initial report of the Attorney General

The first report required to be submitted by the Attorney General under subsection (a) shall include a summary of the efforts, activities, and resources the Department of Justice has allocated in the 5 years prior to October 13, 2008, as well as the 1-year period following such date, to the enforcement, investigation, and prosecution of intellectual property crimes, including—

(1) a review of the policies and efforts of the Department of Justice related to the prevention and investigation of intellectual property crimes, including efforts at the Office of Justice Programs, the Criminal Division of the Department of Justice, the Executive Office of United States Attorneys, the Office of the Attorney General, the Office of the Deputy Attorney General, the Office of Legal Policy, and any other agency or bureau of the Department of Justice whose activities relate to intellectual property;

(2) a summary of the overall successes and failures of such policies and efforts;

(3) a review of the investigative and prosecution activity of the Department of Justice with respect to intellectual property crimes, including—

(A) the number of investigations initiated related to such crimes;

(B) the number of arrests related to such crimes; and

(C) the number of prosecutions for such crimes, including—

(i) the number of defendants involved in such prosecutions;

(ii) whether the prosecution resulted in a conviction; and

(iii) the sentence and the statutory maximum for such crime, as well as the average sentence imposed for such crime; and

(4) a Department-wide assessment of the staff, financial resources, and other resources (such as time, technology, and training) devoted to the enforcement, investigation, and prosecution of intellectual property crimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting intellectual property crimes.

(c) Report of the FBI

Not later than 1 year after October 13, 2008, and annually thereafter, the Director of the Federal Bureau of Investigation shall submit a report to Congress on actions taken to carry out sections 30103 to 30106 of this title. The initial report required under this subsection shall be submitted by May 1, 2009. All subsequent annual

reports shall be submitted by May 1st of each fiscal year thereafter. The report required under this subsection may be submitted as part of the annual performance report of the Department of Justice, and shall include—

(1) a review of the policies and efforts of the Bureau related to the prevention and investigation of intellectual property crimes;

(2) a summary of the overall successes and failures of such policies and efforts;

(3) a review of the investigative and prosecution activity of the Bureau with respect to intellectual property crimes, including—

(A) the number of investigations initiated related to such crimes;

(B) the number of arrests related to such crimes; and

(C) the number of prosecutions for such crimes, including—

(i) the number of defendants involved in such prosecutions;

(ii) whether the prosecution resulted in a conviction; and

(iii) the sentence and the statutory maximum for such crime, as well as the average sentence imposed for such crime; and

(4) a Bureau-wide assessment of the staff, financial resources, and other resources (such as time, technology, and training) devoted to the enforcement, investigation, and prosecution of intellectual property crimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting intellectual property crimes.

(d) Initial report of the FBI

The first report required to be submitted by the Director of the Federal Bureau of Investigation under subsection (c) shall include a summary of the efforts, activities, and resources the Federal Bureau of Investigation has allocated in the 5 years prior to October 13, 2008, as well as the 1-year period following such date to the enforcement, investigation, and prosecution of intellectual property crimes, including—

(1) a review of the policies and efforts of the Bureau related to the prevention and investigation of intellectual property crimes;

(2) a summary of the overall successes and failures of such policies and efforts;

(3) a review of the investigative and prosecution activity of the Bureau with respect to intellectual property crimes, including—

(A) the number of investigations initiated related to such crimes;

(B) the number of arrests related to such crimes; and

(C) the number of prosecutions for such crimes, including—

(i) the number of defendants involved in such prosecutions;

(ii) whether the prosecution resulted in a conviction; and

(iii) the sentence and the statutory maximum for such crime, as well as the average sentence imposed for such crime; and

(4) a Bureau-wide assessment of the staff, financial resources, and other resources (such as time, technology, and training) devoted to the enforcement, investigation, and prosecution of intellectual property crimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting intellectual property crimes.

(Pub. L. 110–403, title IV, § 404, Oct. 13, 2008, 122 Stat. 4274.)

Editorial Notes

REFERENCES IN TEXT

Sections 30103 to 30106 of this title, referred to in subsecs. (a) and (c), was in the original ''this title'', meaning title IV of Pub. L. 110–403, Oct. 13, 2008, 122 Stat. 4271, which enacted sections 30103 to 30106 of this title and amended section 30101 of this title. For complete classification of title IV to the Code, see Tables.

CODIFICATION

Section was formerly classified to section 3713d of Title 42, The Public Health and Welfare, prior to editorial reclassification and renumbering as this section.

§ 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 indi-

viduals 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

(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), establish 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 the United States have faced a heightened risk of cybercrime during the COVID–19 pandemic.

''(4) Subsection (c) of the Uniform Federal Crime Reporting Act of 1988 (34 U.S.C. 41303(c)) requires the Attorney General to 'acquire, collect, classify, and preserve national data on Federal criminal offenses as part of the Uniform Crime Reports' and requires all Federal departments and agencies that investigate criminal activity to 'report details about crime within their respective jurisdiction to the Attorney General in a uniform matter and on a form prescribed by the Attorney General'.

''SEC. 3. CYBERCRIME TAXONOMY.

''(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [May 5, 2022], the Attorney General shall seek to enter into an agreement with the National Academy of Sciences to develop a taxonomy for the purpose of categorizing different types of cybercrime and cyber-enabled crime faced by individuals and businesses.

''(b) DEVELOPMENT.—In developing the taxonomy under subsection (a), the National Academy of Sciences shall—

''(1) ensure the taxonomy is useful for the Federal Bureau of Investigation to classify cybercrime in the National Incident-Based Reporting System, or any successor system;

''(2) consult relevant stakeholders, including—

''(A) the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security;

''(B) Federal, State, and local law enforcement agencies;

''(C) criminologists and academics;

''(D) cybercrime experts; and

''(E) business leaders; and

''(3) take into consideration relevant taxonomies developed by non-governmental organizations, international organizations, academies, or other entities.

''(c) REPORT.—Not later than 1 year after the date on which the Attorney General enters into an agreement under subsection (a), the National Academy of Sciences shall submit to the appropriate committees of Congress, which shall include the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, a report detailing and summarizing—

''(1) the taxonomy developed under subsection (a); and

''(2) any findings from the process of developing the taxonomy under subsection (a).

''(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $1,000,000.

''SEC. 4. CYBERCRIME REPORTING.

''(a) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Attorney General shall establish a category in the National Incident-Based Reporting System, or any successor system, for the collection of cybercrime and cyber-enabled crime reports from Federal, State, and local officials.

''(b) RECOMMENDATIONS.—In establishing the category required under subsection (a), the Attorney General shall, as appropriate, incorporate recommendations from the taxonomy developed under section 3(a).

''SEC. 5. NATIONAL CRIME VICTIMIZATION SURVEY.

''(a) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director of the Bureau of Justice Statistics, in coordination with the Director of the Bureau of the Census, shall include questions relating to cybercrime victimization in the National Crime Victimization Survey.

''(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $2,000,000.

''SEC. 6. GAO STUDY ON CYBERCRIME METRICS.

''Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report that assesses—

''(1) the effectiveness of reporting mechanisms for cybercrime and cyber-enabled crime in the United States; and

''(2) disparities in reporting data between—

''(A) data relating to cybercrime and cyber-enabled crime; and

''(B) other types of crime data.''

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.

§ 30110. Improved investigative and forensic resources for enforcement of laws related to cybercrimes against individuals

Subject to the availability of appropriations to carry out this section, the Attorney General, in consultation with the Director of the Federal Bureau of Investigation and the Secretary of Homeland Security, including the Executive Associate Director of Homeland Security Investigations, shall, with respect to cybercrimes against individuals—

(1) ensure that there are not fewer than 10 additional operational agents of the Federal Bureau of Investigation designated to support the Criminal Division of the Department of Justice in the investigation and coordination of cybercrimes against individuals;

(2) ensure that each office of a United States Attorney designates at least 1 Assistant United States Attorney as responsible for investigating and prosecuting cybercrimes against individuals; and

(3) ensure the implementation of a regular and comprehensive training program—

(A) the purpose of which is to train agents of the Federal Bureau of Investigation in the investigation and prosecution of such crimes and the enforcement of laws related to cybercrimes against individuals; and

(B) that includes relevant forensic training related to investigating and prosecuting cybercrimes against individuals.

(Pub. L. 117–347, title III, § 321, Jan. 5, 2023, 136 Stat. 6206.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of ''cybercrime against individuals'' as used in this section, 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.

§ 30111. Training and technical assistance for States

The Attorney General, in consultation with the Secretary of Homeland Security, the Director of the United States Secret Service, the Executive Associate Director of Homeland Security Investigations, and nongovernmental and survivor stakeholders, shall create, compile, evaluate, and disseminate materials and information, and provide the necessary training and technical assistance, to assist States and units of local government in—

(1) investigating, prosecuting, pursuing, preventing, understanding, and mitigating the impact of—

(A) physical, sexual, and psychological abuse of cybercrime victims, including victims of human trafficking that is facilitated by interactive computer services;

(B) exploitation of cybercrime victims; and

(C) deprioritization of cybercrime; and

(2) assessing, addressing, and mitigating the physical and psychological trauma to victims of cybercrime.

(Pub. L. 117–347, title III, § 324, Jan. 5, 2023, 136 Stat. 6207.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of ''computer'' as used in this section, see section 3 of Pub. L. 117–347, set out as a note under section 20145 of this title.

CHAPTER 303—PRISON RAPE ELIMINATION

§ 30301. Findings

Congress makes the following findings:

(1) 2,100,146 persons were incarcerated in the United States at the end of 2001: 1,324,465 in Federal and State prisons and 631,240 in county and local jails. In 1999, there were more than 10,000,000 separate admissions to and discharges from prisons and jails.

(2) Insufficient research has been conducted and insufficient data reported on the extent of prison rape. However, experts have conservatively estimated that at least 13 percent of the inmates in the United States have been