AMENDMENT TO RULES COMMITTEE PRINT 116-9

OFFERED BY MS. CLARK OF MASSACHUSETTS

Add, at the end of the bill, the following (and conform the table of contents accordingly):

TITLE XV—CYBERCRIME ENFORCEMENT

SEC. 1501. LOCAL LAW ENFORCEMENT GRANTS FOR ENFORCEMENT OF CYBERCRIMES.

(a) IN GENERAL.—Subject to the availability of appropriations, the Attorney General shall award grants under this section to States and units of local government for the prevention, enforcement, and prosecution of cybercrimes against individuals.

(b) APPLICATION.—

(1) IN GENERAL.—To request a grant under this section, the chief executive officer of a State or unit of local government shall submit an application to the Attorney General within 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. Such application shall include the following:

(A) A certification that Federal funds made available under this section will not be used to supplant State 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 fewer 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 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 and to neighborhood or community-based organizations, 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 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 (c)(7) 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.

(c) USE OF FUNDS.—Grants awarded under this section may only be used for programs that provide—

(1) training for State or local law enforcement 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, 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 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, 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 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, 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 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 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 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;

(7) assistance to State or local law enforcement 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;

(8) assistance in the facilitation and promotion of 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 laws that prohibit cybercrimes against individuals, including the use of multijurisdictional task forces; or

(9) assistance to State 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.

(d) REPORT TO THE SECRETARY.—On the date that is one year after the date on which a State or unit of local

government receives a grant under this section, and annually thereafter, the chief executive of such State 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 by such State 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.

(e) REPORT 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 report submitted under subsection (d).

(f) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated to carry out this section $20,000,000 for each of fiscal years 2020 through 2024.

(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.

(g) DEFINITIONS.—In this section:

(1) The term ''cybercrimes against individuals'' means the criminal offenses applicable in the relevant State or unit of local government that involve the use of a computer to cause personal harm to an individual, such as the use of a computer to harass, threaten, stalk, extort, coerce, cause fear, intimidate, without consent distribute intimate images of, or violate the privacy of, an individual, except that—

(A) use of a computer need not be an element of such an offense; and

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

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

SEC. 1502. NATIONAL RESOURCE CENTER GRANT.

(a) IN GENERAL.—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 pro-

vide 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.

(b) APPLICATION.—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 2020 in such form as the Attorney General may require. Such application shall include the following:

(1) 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.

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

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

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

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

(c) 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 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.

(d) DURATION OF GRANT.—

(1) IN GENERAL.—The 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 (c), and if the recipient resubmits an application described in subsection (b) in such form, and at such time as the Attorney General may reasonably require.

(e) 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 (c).

(f) REPORT TO THE SECRETARY.—On the date that is one year after the date on which an eligible entity re-

ceives 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.

(g) REPORT 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 report submitted under subsection (d).

(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $4,000,000 for each of fiscal years 2020 through 2024.

(i) DEFINITIONS.—In this section:

(1) CYBERCRIMES AGAINST INDIVIDUALS.—The term ''cybercrimes against individuals'' has the meaning given such term in section 1501(g).

(2) ELIGIBLE ENTITY.—The term ''eligible entity'' means a nonprofit private organization that focuses on cybercrimes against individuals and that—

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

(B) includes on the entity's advisory board representatives who have a documented history of working directly on issues of cybercrimes against individuals and who are geographically and culturally diverse.

SEC. 1503. 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'' means a Federal, State, or local criminal offense that involves the use of a computer to cause personal harm to an individual, such as the use of a computer to harass, threaten, stalk, extort, coerce, cause fear, intimidate,

without consent distribute intimate images of, or violate the privacy of, an individual, except that—

(A) use of a computer need not be an element of the offense; and

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

(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; and

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

(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, United States Code, 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.

☒