

**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):

1                   **TITLE XV—CYBERCRIME**  
2                   **ENFORCEMENT**

3 **SEC. 1501. LOCAL LAW ENFORCEMENT GRANTS FOR EN-**  
4                   **FORCEMENT OF CYBERCRIMES.**

5           (a) IN GENERAL.—Subject to the availability of ap-  
6 propriations, the Attorney General shall award grants  
7 under this section to States and units of local government  
8 for the prevention, enforcement, and prosecution of  
9 cybercrimes against individuals.

10           (b) APPLICATION.—

11               (1) IN GENERAL.—To request a grant under  
12 this section, the chief executive officer of a State or  
13 unit of local government shall submit an application  
14 to the Attorney General within 90 days after the  
15 date on which funds to carry out this section are ap-  
16 propriated for a fiscal year, in such form as the At-  
17 torney General may require. Such application shall  
18 include the following:

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

7 (B) An assurance that, not fewer than 30  
8 days before the application (or any amendment  
9 to the application) was submitted to the Attor-  
10 ney General, the application (or amendment)  
11 was submitted for review to the governing body  
12 of the State or unit of local government (or to  
13 an organization designated by that governing  
14 body).

15 (C) An assurance that, before the applica-  
16 tion (or any amendment to the application) was  
17 submitted to the Attorney General—

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

20 (ii) an opportunity to comment on the  
21 application (or amendment) was provided  
22 to citizens and to neighborhood or commu-  
23 nity-based organizations, to the extent ap-  
24 plicable law or established procedure  
25 makes such an opportunity available.

1 (D) An assurance that, for each fiscal year  
2 covered by an application, the applicant shall  
3 maintain and report such data, records, and in-  
4 formation (programmatic and financial) as the  
5 Attorney General may reasonably require.

6 (E) A certification, made in a form accept-  
7 able to the Attorney General and executed by  
8 the chief executive officer of the applicant (or  
9 by another officer of the applicant, if qualified  
10 under regulations promulgated by the Attorney  
11 General), that—

12 (i) the programs to be funded by the  
13 grant meet all the requirements of this sec-  
14 tion;

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

17 (iii) there has been appropriate co-  
18 ordination with affected agencies; and

19 (iv) the applicant will comply with all  
20 provisions of this section and all other ap-  
21 plicable Federal laws.

22 (F) A certification that the State or in the  
23 case of a unit of local government, the State in  
24 which the unit of local government is located,

1 has in effect criminal laws which prohibit  
2 cybercrimes against individuals.

3 (G) A certification that any equipment de-  
4 scribed in subsection (e)(7) purchased using  
5 grant funds awarded under this section will be  
6 used primarily for investigations and forensic  
7 analysis of evidence in matters involving  
8 cybercrimes against individuals.

9 (e) USE OF FUNDS.—Grants awarded under this sec-  
10 tion may only be used for programs that provide—

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

14 (A) training such personnel to identify and  
15 protect victims of cybercrimes against individ-  
16 uals;

17 (B) training such personnel to utilize Fed-  
18 eral, State, local, and other resources to assist  
19 victims of cybercrimes against individuals;

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

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

1 (E) training such personnel to utilize tech-  
2 nology to assist in the investigation of  
3 cybercrimes against individuals and enforce-  
4 ment of laws that prohibit such crimes; and

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

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

10 (A) training such personnel to identify, in-  
11 vestigate, prosecute, or adjudicate cybercrimes  
12 against individuals;

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

15 (C) training such personnel to utilize Fed-  
16 eral, State, local, and other resources to assist  
17 victims of cybercrimes against individuals; and

18 (D) training such personnel to utilize tech-  
19 nology to assist in the prosecution or adjudica-  
20 tion of acts of cybercrimes against individuals,  
21 including the use of technology to protect vic-  
22 tims of such crimes;

23 (3) training for State or local emergency dis-  
24 patch personnel relating to cybercrimes against indi-  
25 viduals, including—

1 (A) training such personnel to identify and  
2 protect victims of cybercrimes against individ-  
3 uals;

4 (B) training such personnel to utilize Fed-  
5 eral, State, local, and other resources to assist  
6 victims of cybercrimes against individuals;

7 (C) training such personnel to utilize tech-  
8 nology to assist in the identification of and re-  
9 sponse to cybercrimes against individuals; and

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

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

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

21 (6) assistance to State or local law enforcement  
22 agencies to establish task forces that operate solely  
23 to conduct investigations, forensic analyses of evi-  
24 dence, and prosecutions in matters involving  
25 cybercrimes against individuals;

1           (7) assistance to State or local law enforcement  
2           and prosecutors in acquiring computers, computer  
3           equipment, and other equipment necessary to con-  
4           duct investigations and forensic analysis of evidence  
5           in matters involving cybercrimes against individuals,  
6           including expenses incurred in the training, mainte-  
7           nance, or acquisition of technical updates necessary  
8           for the use of such equipment for the duration of a  
9           reasonable period of use of such equipment;

10           (8) assistance in the facilitation and promotion  
11           of sharing, with State and local law enforcement of-  
12           ficers and prosecutors, of the expertise and informa-  
13           tion of Federal law enforcement agencies about the  
14           investigation, analysis, and prosecution of matters  
15           involving laws that prohibit cybercrimes against indi-  
16           viduals, including the use of multijurisdictional task  
17           forces; or

18           (9) assistance to State and local law enforce-  
19           ment and prosecutors in processing interstate extra-  
20           dition requests for violations of laws involving  
21           cybercrimes against individuals, including expenses  
22           incurred in the extradition of an offender from one  
23           State to another.

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

1 government receives a grant under this section, and annu-  
2 ally thereafter, the chief executive of such State or unit  
3 of local government shall submit to the Attorney General  
4 a report which contains—

5 (1) a summary of the activities carried out dur-  
6 ing the previous year with any grant received by  
7 such State or unit of local government;

8 (2) an evaluation of the results of such activi-  
9 ties; and

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

12 (e) REPORT TO CONGRESS.—Not later than Novem-  
13 ber 1 of each even-numbered fiscal year, the Attorney  
14 General shall submit to the Committee on the Judiciary  
15 of the House of Representatives and the Committee on  
16 the Judiciary of the Senate a report that contains a com-  
17 pilation of the information contained in the report sub-  
18 mitted under subsection (d).

19 (f) AUTHORIZATION OF APPROPRIATIONS.—

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

23 (2) LIMITATION.—Of the amount made avail-  
24 able under paragraph (1) in any fiscal year, not  
25 more than 5 percent may be used for evaluation,



1 monitoring, technical assistance, salaries, and ad-  
2 ministrative expenses.

3 (g) DEFINITIONS.—In this section:

4 (1) The term “cybercrimes against individuals”  
5 means the criminal offenses applicable in the rel-  
6 evant State or unit of local government that involve  
7 the use of a computer to cause personal harm to an  
8 individual, such as the use of a computer to harass,  
9 threaten, stalk, extort, coerce, cause fear, intimidate,  
10 without consent distribute intimate images of, or vio-  
11 late the privacy of, an individual, except that—

12 (A) use of a computer need not be an ele-  
13 ment of such an offense; and

14 (B) such term does not include the use of  
15 a computer to cause harm to a commercial enti-  
16 ty, government agency, or any non-natural per-  
17 sons.

18 (2) The term “computer” includes a computer  
19 network and an interactive electronic device.

20 **SEC. 1502. NATIONAL RESOURCE CENTER GRANT.**

21 (a) IN GENERAL.—Subject to the availability of ap-  
22 propriations, the Attorney General shall award a grant  
23 under this section to an eligible entity for the purpose of  
24 the establishment and maintenance of a National Re-  
25 source Center on Cybercrimes Against Individuals to pro-

1 vide resource information, training, and technical assist-  
2 ance to improve the capacity of individuals, organizations,  
3 governmental entities, and communities to prevent, en-  
4 force, and prosecute cybercrimes against individuals.

5 (b) APPLICATION.—To request a grant under this  
6 section, an eligible entity shall submit an application to  
7 the Attorney General not later than 90 days after the date  
8 on which funds to carry out this section are appropriated  
9 for fiscal year 2020 in such form as the Attorney General  
10 may require. Such application shall include the following:

11 (1) An assurance that, for each fiscal year cov-  
12 ered by an application, the applicant shall maintain  
13 and report such data, records, and information (pro-  
14 grammatic and financial) as the Attorney General  
15 may reasonably require.

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

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

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

22 (C) the applicant will comply with all pro-  
23 visions of this section and all other applicable  
24 Federal laws.

1           (c) USE OF FUNDS.—The eligible entity awarded a  
2 grant under this section shall use such amounts for the  
3 establishment and maintenance of a National Resource  
4 Center on Cybercrimes Against Individuals, which shall—

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

11           (2) maintain a resource library which shall col-  
12 lect, prepare, analyze, and disseminate information  
13 and statistics related to—

14           (A) the incidence of cybercrimes against  
15 individuals;

16           (B) the enforcement, and prosecution of  
17 laws relating to cybercrimes against individuals;  
18 and

19           (C) the provision of supportive services and  
20 resources for victims of cybercrimes against in-  
21 dividuals; and

22           (3) conduct research related to—

23           (A) the causes of cybercrimes against indi-  
24 viduals;

1 (B) the effect of cybercrimes against indi-  
2 viduals on victims of such crimes; and

3 (C) model solutions to prevent or deter  
4 cybercrimes against individuals or to enforce  
5 the laws relating to cybercrimes against individ-  
6 uals.

7 (d) DURATION OF GRANT.—

8 (1) IN GENERAL.—The grant awarded under  
9 this section shall be awarded for a period of 5 years.

10 (2) RENEWAL.—A grant under this section may  
11 be renewed for additional 5-year periods if the At-  
12 torney General determines that the funds made  
13 available to the recipient were used in a manner de-  
14 scribed in subsection (c), and if the recipient resub-  
15 mits an application described in subsection (b) in  
16 such form, and at such time as the Attorney General  
17 may reasonably require.

18 (e) SUBGRANTS.—The eligible entity awarded a grant  
19 under this section may make subgrants to other nonprofit  
20 private organizations with relevant subject matter exper-  
21 tise in order to establish and maintain the National Re-  
22 source Center on Cybercrimes Against Individuals in ac-  
23 cordance with subsection (c).

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

1 ceives a grant under this section, and annually thereafter  
2 for the duration of the grant period, the entity shall sub-  
3 mit to the Attorney General a report which contains—

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

6 (2) an evaluation of the results of such activi-  
7 ties; and

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

10 (g) REPORT TO CONGRESS.—Not later than Novem-  
11 ber 1 of each even-numbered fiscal year, the Attorney  
12 General shall submit to the Committee on the Judiciary  
13 of the House of Representatives and the Committee on  
14 the Judiciary of the Senate a report that contains a com-  
15 pilation of the information contained in the report sub-  
16 mitted under subsection (d).

17 (h) AUTHORIZATION OF APPROPRIATIONS.—There  
18 are authorized to be appropriated to carry out this section  
19 \$4,000,000 for each of fiscal years 2020 through 2024.

20 (i) DEFINITIONS.—In this section:

21 (1) CYBERCRIMES AGAINST INDIVIDUALS.—The  
22 term “cybercrimes against individuals” has the  
23 meaning given such term in section 1501(g).

1           (2) ELIGIBLE ENTITY.—The term “eligible enti-  
2           ty” means a nonprofit private organization that fo-  
3           cuses on cybercrimes against individuals and that—

4                   (A) provides documentation to the Attor-  
5           ney General demonstrating experience working  
6           directly on issues of cybercrimes against indi-  
7           viduals; and

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

13 **SEC. 1503. NATIONAL STRATEGY, CLASSIFICATION, AND RE-**  
14 **PORTING ON CYBERCRIME.**

15          (a) DEFINITIONS.—In this section:

16               (1) COMPUTER.—The term “computer” in-  
17               cludes a computer network and any interactive elec-  
18               tronic device.

19               (2) CYBERCRIME AGAINST INDIVIDUALS.—The  
20               term “cybercrime against individuals” means a Fed-  
21               eral, State, or local criminal offense that involves the  
22               use of a computer to cause personal harm to an in-  
23               dividual, such as the use of a computer to harass,  
24               threaten, stalk, extort, coerce, cause fear, intimidate,

1 without consent distribute intimate images of, or vio-  
2 late the privacy of, an individual, except that—

3 (A) use of a computer need not be an ele-  
4 ment of the offense; and

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

8 (b) NATIONAL STRATEGY.—The Attorney General  
9 shall develop a national strategy to—

10 (1) reduce the incidence of cybercrimes against  
11 individuals;

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

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

17 (c) CLASSIFICATION OF CYBERCRIMES AGAINST IN-  
18 DIVIDUALS FOR PURPOSES OF CRIME REPORTS.—In ac-  
19 cordance with the authority of the Attorney General under  
20 section 534 of title 28, United States Code, the Director  
21 of the Federal Bureau of Investigation shall—

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

1           (2) to the extent feasible, within the category  
2           established under paragraph (1), establish subcat-  
3           egories for each type of cybercrime against individ-  
4           uals that is an offense under Federal or State law;

5           (3) classify the category established under para-  
6           graph (1) as a Part I crime in the Uniform Crime  
7           Reports; and

8           (4) classify each type of cybercrime against in-  
9           dividuals that is an offense under Federal or State  
10          law as a Group A offense for the purpose of the Na-  
11          tional Incident-Based Reporting System.

12          (d) ANNUAL SUMMARY.—The Attorney General shall  
13          publish an annual summary of the information reported  
14          in the Uniform Crime Reports and the National Incident-  
15          Based Reporting System relating to cybercrimes against  
16          individuals.

