

116TH CONGRESS  
1ST SESSION

# H. R. 5227

To establish the Office of Digital Law Enforcement within the Office of Justice Programs, and to establish grant programs to improve the digital evidence capacity of law enforcement personnel, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 21, 2019

Mrs. DEMINGS (for herself, Mr. LAMB, Mr. RUTHERFORD, and Mr. BABIN) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## A BILL

To establish the Office of Digital Law Enforcement within the Office of Justice Programs, and to establish grant programs to improve the digital evidence capacity of law enforcement personnel, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Technology in Criminal  
5 Justice Act of 2019”.

1 **SEC. 2. OFFICE OF DIGITAL LAW ENFORCEMENT.**

2 Part A of title I of the Omnibus Crime Control and  
3 Safe Streets Act of 1968 (34 U.S.C. 10101 et seq.) is  
4 amended by adding at the end the following:

5 **“SEC. 110. OFFICE OF DIGITAL LAW ENFORCEMENT.**

6 “(a) ESTABLISHMENT.—There is established within  
7 the Office an Office of Digital Law Enforcement, which  
8 shall headed by a Director appointed by the Attorney Gen-  
9 eral. In carrying out the functions of the Office of Digital  
10 Law Enforcement, the Director shall be subject to the au-  
11 thority, direction, and control of the Attorney General.  
12 Such authority, direction, and control may be delegated  
13 only to the Assistant Attorney General.

14 “(b) PURPOSE.—The purpose of the Office of Digital  
15 Law Enforcement shall be to support Federal, State, and  
16 local law enforcement in training, preparing, and sup-  
17 porting criminal justice personnel in the conduct of crimi-  
18 nal justice activities utilizing digital evidence.

19 “(c) GRANTS.—

20 “(1) IN GENERAL.—In carrying out the purpose  
21 described under subsection (b), the Director may  
22 make grants to eligible recipients.

23 “(2) USES.—Grants awarded under this sub-  
24 section shall be used to support the provision of  
25 training, education, and technical assistance to  
26 criminal justice personnel for the purpose of improv-

1 ing the digital evidence capacity (as such term is de-  
2 fined in section 7 of the Technology in Criminal Jus-  
3 tice Act of 2019) of law enforcement personnel (as  
4 such term is defined in section 7 of the Technology  
5 in Criminal Justice Act of 2019).

6 “(3) DISTRIBUTION.—In making grants under  
7 this subsection, the Director shall ensure that, to the  
8 extent practicable, distribution of such grants en-  
9 sures equitable access to relevant training, edu-  
10 cation, and technical assistance across geographic  
11 areas and across urban and rural areas of varying  
12 population and area.

13 “(4) ELIGIBLE RECIPIENTS.—The Director  
14 may award grants under this subsection to the fol-  
15 lowing eligible recipients:

16 “(A) The National Domestic Communica-  
17 tions Assistance Center (NDCAC).

18 “(B) The National Computer Forensics In-  
19 stitute (NCFI).

20 “(C) The Law Enforcement Cyber Center.

21 “(D) The National White Collar Crime  
22 Center (NW3C).

23 “(E) The National Cyber-Forensics and  
24 Training Alliance (NCF'TA).

1                   “(F) Regional Computer Forensics Lab-  
2                   ratories.

3                   “(G) Such other entities as the Director  
4                   deems appropriate.

5           “(d) STANDARDIZATION OF TRAINING CURRICULA.—  
6 The Director shall—

7                   “(1) on an ongoing basis, review curricula used  
8                   for training and education programs supported by  
9                   grants under subsection (c);

10                   “(2) identify opportunities for standardization  
11                   of such curricula; and

12                   “(3) in awarding grants under subsection (c),  
13                   establish requirements or processes, as appropriate,  
14                   to promote standardization of such curricula.

15           “(e) BEST PRACTICES.—The Director shall—

16                   “(1) identify best practices relevant to digital  
17                   evidence capacity; and

18                   “(2) develop mechanisms to inform Federal,  
19                   State, and local criminal justice personnel of such  
20                   best practices and promote their adoption.

21           “(f) DATA ON LAW ENFORCEMENT ACCESS TO DIG-  
22 ITAL EVIDENCE.—The Director shall—

23                   “(1) maintain data relevant to digital evidence  
24                   capacity, including challenges to accessing and uti-

1 lizing digital evidence and digital forensic laboratory  
2 backlogs; and

3 “(2) no later than January 31 of each calendar  
4 year, submit to Congress a report summarizing data  
5 collected under paragraph (f)(1) of this section dur-  
6 ing the preceding calendar year and identifying key  
7 trends, gaps, and challenges associated with the  
8 data. The report shall be submitted in unclassified  
9 format.”.

10 **SEC. 3. REVIEW OF FEDERAL SUPPORT FOR DIGITAL LAW**  
11 **ENFORCEMENT TRAINING AND ASSISTANCE.**

12 (a) **REVIEW REQUIRED.**—The Attorney General and  
13 the Secretary of Homeland Security shall jointly conduct  
14 a review of existing United States Government programs  
15 that provide training, education, and technical assistance  
16 to criminal justice personnel for the purpose of improving  
17 digital evidence capacity.

18 (b) **ELEMENTS OF REVIEW.**—The review required  
19 under subsection (a) shall examine the following matters:

20 (1) Identification of existing programs that pro-  
21 vide training, education, and technical assistance to  
22 criminal justice personnel, and the sources and  
23 amounts of U.S. Government funding supporting  
24 such programs, for the purpose of improving the

1 digital evidence capacity of law enforcement per-  
2 sonnel.

3 (2) Examination of the purposes, organizational  
4 models, target audiences, and effectiveness of these  
5 programs.

6 (3) Identification of gaps in these programs,  
7 and assessment of whether these programs are suffi-  
8 cient to meet the needs of Federal, State, and local  
9 criminal justice personnel.

10 (4) Recommendations for opportunities, if any,  
11 to improve these programs in order to achieve great-  
12 er efficiency, coherence, or effectiveness in the deliv-  
13 ery of such training, education, and technical assist-  
14 ance, including through expansion, consolidation, or  
15 reorganization.

16 (c) REPORT TO CONGRESS.—Upon completion of the  
17 review required in subsection (a), and not later than 360  
18 days after the enactment of this Act, the Attorney General  
19 and the Secretary of Homeland Security shall submit to  
20 Congress a joint report summarizing the conclusions of  
21 the review and providing any recommendations to Con-  
22 gress for legislative action.

23 **SEC. 4. CENTER OF EXCELLENCE FOR DIGITAL FORENSICS.**

24 (a) DESIGNATION.—Not later than 360 days after  
25 the enactment of this Act, the Attorney General, in con-

1 sultation with the Secretary of Homeland Security, shall  
2 designate an entity of the Federal Government as the Cen-  
3 ter of Excellence for Digital Forensics (hereafter, the  
4 “Center”).

5 (b) MISSION.—The Center shall be a clearinghouse  
6 for training, technical expertise, and legal assistance relat-  
7 ing to accessing digital evidence in support of criminal in-  
8 vestigations, including by—

9 (1) serving as a central repository of knowledge  
10 and expertise regarding common types of data rel-  
11 evant to law enforcement investigations, common  
12 technical systems for storing and transmitting such  
13 data, formulation of lawful requests for such data,  
14 and procedures for submitting such requests;

15 (2) building and maintaining a library of ana-  
16 lytic and forensic tools, along with technical exper-  
17 tise on the use of such tools, to be available to sup-  
18 port Federal, State, and local law enforcement inves-  
19 tigations;

20 (3) developing and maintaining technical sup-  
21 port tools to facilitate, standardize, and authenticate  
22 law enforcement requests for digital evidence;

23 (4) providing training to Federal, State, and  
24 local law enforcement organizations on procedures  
25 and techniques for the acquisition, exploitation, pres-

1       ervation, and utilization of digital evidence, as well  
2       as the protection of privacy and civil liberties in the  
3       course of investigations and prosecutions involving  
4       digital evidence;

5           (5) producing and maintaining up-to-date train-  
6       ing materials and curricula to support training of  
7       Federal, State, and local law enforcement organiza-  
8       tions relating to digital evidence capacity by other  
9       training providers;

10          (6) coordinating with international, Federal,  
11       and State training programs, as well as relevant  
12       non-governmental stakeholders, to leverage and co-  
13       ordinate existing resources for training, technical as-  
14       sistance tools, and informative materials on proce-  
15       dures and techniques relating to digital evidence ca-  
16       pacity; and

17          (7) providing a hotline available for law enforce-  
18       ment officials seeking advice about or assistance re-  
19       lating to digital evidence capacity.

20       (c) COORDINATION WITH EXISTING TRAINING PRO-  
21       VIDERS.—The designation required by subsection (a) shall  
22       be informed by the results of the review conducted under  
23       section 3.

24       (d) TERMINATION OR MODIFICATION OF DESIGNA-  
25       TION.—The Attorney General may terminate or modify

1 the designation under subsection (a) if the Attorney Gen-  
2 eral, in consultation with the Secretary of Homeland Secu-  
3 rity, determines that the Center is no longer capable of  
4 achieving the missions specified in subsection (b) and des-  
5 ignates a separate entity of the Federal Government to  
6 serve as the Center. Not later than 60 days before the  
7 effective date of such a termination, the Secretary shall  
8 provide written notice to Congress, including the rationale  
9 for such termination.

10 **SEC. 5. FEDERAL GOVERNMENT LAW ENFORCEMENT TECH-**  
11 **NOLOGY SUPPORT TO STATE AND LOCAL**  
12 **LAW ENFORCEMENT.**

13 (a) PROGRAM.—The Attorney General and the Sec-  
14 retary of Homeland Security shall jointly establish a Law  
15 Enforcement Technology Support to State and Local Law  
16 Enforcement program under the direction of the Director  
17 of the Office of Digital Law Enforcement.

18 (b) DEVELOPMENT.—Under the program established  
19 in subsection (a), the Attorney General and the Secretary  
20 shall jointly develop guidelines and processes, as appro-  
21 priate, to authorize the use of funds made available to  
22 grantees under the following programs for purposes of ac-  
23 quiring technology to improve the digital evidence capacity  
24 of law enforcement personnel:

1           (1) The Edward Byrne Memorial Justice As-  
2           sistance Grant program.

3           (2) The Urban Area Security Initiative.

4           (3) The State Homeland Security Grant Pro-  
5           gram.

6           (c) DISSEMINATION OF ACQUISITION GUIDANCE.—

7 Through the program established in subsection (a), the  
8 Attorney General and the Secretary shall develop guidance  
9 on acquisition of law enforcement technologies that sup-  
10 port digital evidence capacity, and regularly disseminate  
11 such guidance to State and local law enforcement organi-  
12 zations. Such guidance shall identify and encourage adop-  
13 tion of effective law enforcement technologies useful across  
14 different technological platforms and formats.

15           (d) PUBLIC-PRIVATE PARTNERSHIPS.—Subject to  
16 the availability of resources, the Attorney General and the  
17 Secretary shall, under the program established in sub-  
18 section (a), enter into partnerships with public or private  
19 entities to improve the access of Federal, State, and local  
20 law enforcement personnel to law enforcement tech-  
21 nologies that support digital evidence capacity. Such part-  
22 nerships may—

23           (1) develop collaborative approaches to devel-  
24           oping new investigative tools;

1           (2) promote the exchange of technical experts  
2           between the technology and law enforcement commu-  
3           nities;

4           (3) build public access data sets that may aid  
5           law enforcement investigations;

6           (4) exchange information on technical ap-  
7           proaches relating to digital evidence capacity, con-  
8           sistent with relevant laws and policies;

9           (5) develop training modules and content to  
10          support training of criminal justice personnel on rel-  
11          evant topics relating to digital evidence capacity; and

12          (6) address other such matters as the Attorney  
13          General and the Secretary deem appropriate.

14 **SEC. 6. DEPARTMENT OF JUSTICE TECHNOLOGY POLICY**  
15 **ADVISORY BOARD.**

16          (a) **ESTABLISHMENT.**—There is established a De-  
17          partment of Justice Technology Policy Advisory Board  
18          (hereinafter in this section referred to as the “Board”),  
19          which shall be composed of 11 members appointed in ac-  
20          cordance with subsection (c) and shall conduct its business  
21          in accordance with this chapter.

22          (b) **PURPOSE.**—The purpose of the Board shall be  
23          to—

1           (1) foster sustained dialogue between the tech-  
2 nology and law enforcement communities on policy  
3 issues of mutual concern; and

4           (2) advise the Attorney General on—

5                 (A) relevant developments in technologies  
6 relating to law enforcement, forensics, commu-  
7 nications, and cybersecurity, and their implica-  
8 tions for the Department of Justice;

9                 (B) strategies and technical approaches for  
10 improving digital evidence capacity;

11                (C) strategies and technical approaches for  
12 improving law enforcement activities relating to  
13 the prevention, investigation, and prosecution of  
14 cyber crime; and

15                (D) such other matters as requested by the  
16 Attorney General.

17       (c) MEMBERS.—

18           (1) MEMBERS.—The members of the Board  
19 shall be senior non-government leaders with knowl-  
20 edge or expertise, whether by experience or training,  
21 in the fields of technology, communications, com-  
22 puter science, cybersecurity, digital forensics, law en-  
23 forcement, relevant laws relating to digital searches  
24 and the use of digital evidence, and related fields,  
25 who shall be appointed by the Attorney General.

1           (2) TERM.—The term of a Board member shall  
2 be 4 years.

3           (3) VACANCIES.—Any vacancy in the member-  
4 ship of the Board shall not affect the powers of the  
5 Board and shall be filled in the same manner as the  
6 original appointment.

7           (4) CHAIRMAN.—The Members of the Board  
8 shall elect one member to serve as Chairman of the  
9 Board.

10 (d) COMPENSATION AND EXPENSES.—

11           (1) COMPENSATION.—A Member of the Board  
12 shall receive no compensation for the member's serv-  
13 ices as such.

14           (2) EXPENSES.—A member of the Board shall  
15 be allowed necessary travel expenses (or in the alter-  
16 native, mileage for use of a privately owned vehicle  
17 and a per diem in lieu of subsistence not to exceed  
18 the rate and amount prescribed in sections 5702 and  
19 5704 of title 5, United States Code), and other nec-  
20 essary expenses incurred by the member in the per-  
21 formance of duties vested in the Panel, without re-  
22 gard to the provisions of subchapter I of chapter 57  
23 of title 5, United States Code, the Standardized  
24 Government Travel Regulations, or section 5731 of  
25 title 5, United States Code.

1 (e) SUPPORT.—The Attorney General shall provide  
2 support for the performance of the Board’s functions and  
3 shall ensure compliance with the requirements of the Fed-  
4 eral Advisory Committee Act of 1972 (5 U.S.C., Appen-  
5 dix), the Government in the Sunshine Act of 1976 (5  
6 U.S.C. 552b), governing Federal statutes and regulations,  
7 and Department of Justice policies and procedures.

8 **SEC. 7. DEFINITIONS.**

9 For purposes of this Act:

10 (1) DIGITAL EVIDENCE CAPACITY.—The term  
11 “digital evidence capacity” shall include, in inves-  
12 tigation and prosecutions involving digital evidence,  
13 the capacity, or activities supporting the capacity,  
14 to—

15 (A) acquire digital evidence in accordance  
16 with current surveillance, civil rights, and crimi-  
17 nal justice laws;

18 (B) ensure digital evidence acquisition ac-  
19 tivities—

20 (i) minimize the acquisition of digital  
21 information not necessary to an investiga-  
22 tion, including the acquisition of informa-  
23 tion pertaining to non-targeted persons;

24 (ii) are conducted in accordance with  
25 proper legal processes such as warrants,

1 court orders, and notice when required;

2 and

3 (iii) favor less intrusive investigative

4 techniques when they would suffice;

5 (C) handle and preserve digital evidence

6 appropriately, including by ensuring—

7 (i) the integrity of the evidentiary

8 chain of custody;

9 (ii) preventing inadvertent corruption

10 or destruction of the evidence; and

11 (iii) promoting the prompt return of

12 seized digital devices and the prompt re-

13 turn or destruction of seized digital infor-

14 mation not used in prosecution of the

15 crime for which it was acquired;

16 (D) extract, analyze, and exploit digital

17 evidence;

18 (E) ensure the appropriate use of digital

19 evidence, including by limiting the repurposing

20 of seized digital information;

21 (F) use digital evidence in criminal legal

22 proceedings; and

23 (G) ensure appropriate protections relating

24 to privacy and security are applied to activities

1           involving the acquisition, preservation, analysis  
2           and exploitation, and use of digital information.

3           (2) CRIMINAL JUSTICE PERSONNEL.—The term  
4           “criminal justice personnel” shall mean employees of  
5           any unit of Federal, State, or local government who  
6           have responsibilities pertaining to criminal justice,  
7           as defined by section (a)(1) of title 34, United  
8           States Code.

○