I

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Technology in Criminal Justice Act of 2019''.

SEC. 2. OFFICE OF DIGITAL LAW ENFORCEMENT.

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

"SEC. 110. OFFICE OF DIGITAL LAW ENFORCEMENT.

''(a) ESTABLISHMENT.—There is established within the Office an Office of Digital Law Enforcement, which shall headed by a Director appointed by the Attorney General. In carrying out the functions of the Office of Digital Law Enforcement, the Director shall be subject to the authority, direction, and control of the Attorney General. Such authority, direction, and control may be delegated only to the Assistant Attorney General.

''(b) PURPOSE.—The purpose of the Office of Digital Law Enforcement shall be to support Federal, State, and local law enforcement in training, preparing, and supporting criminal justice personnel in the conduct of criminal justice activities utilizing digital evidence.

''(c) GRANTS.—

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

''(2) USES.—Grants awarded under this subsection shall be used to support the provision of training, education, and technical assistance to criminal justice personnel for the purpose of improv-

ing the digital evidence capacity (as such term is defined in section 7 of the Technology in Criminal Justice Act of 2019) of law enforcement personnel (as such term is defined in section 7 of the Technology in Criminal Justice Act of 2019).

''(3) DISTRIBUTION.—In making grants under this subsection, the Director shall ensure that, to the extent practicable, distribution of such grants ensures equitable access to relevant training, education, and technical assistance across geographic areas and across urban and rural areas of varying population and area.

''(4) ELIGIBLE RECIPIENTS.—The Director may award grants under this subsection to the following eligible recipients:

''(A) The National Domestic Communications Assistance Center (NDCAC).

''(B) The National Computer Forensics Institute (NCFI).

''(C) The Law Enforcement Cyber Center.

''(D) The National White Collar Crime Center (NW3C).

''(E) The National Cyber-Forensics and Training Alliance (NCFTA).

''(F) Regional Computer Forensics Laboratories.

''(G) Such other entities as the Director deems appropriate.

''(d) STANDARDIZATION OF TRAINING CURRICULA.—The Director shall—

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

''(2) identify opportunities for standardization of such curricula; and

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

''(e) BEST PRACTICES.—The Director shall—

''(1) identify best practices relevant to digital evidence capacity; and

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

''(f) DATA ON LAW ENFORCEMENT ACCESS TO DIGITAL EVIDENCE.—The Director shall—

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

lizing digital evidence and digital forensic laboratory backlogs; and

''(2) no later than January 31 of each calendar year, submit to Congress a report summarizing data collected under paragraph (f)(1) of this section during the preceding calendar year and identifying key trends, gaps, and challenges associated with the data. The report shall be submitted in unclassified format.''.

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

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

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

(1) Identification of existing programs that provide training, education, and technical assistance to criminal justice personnel, and the sources and amounts of U.S. Government funding supporting such programs, for the purpose of improving the

digital evidence capacity of law enforcement personnel.

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

(3) Identification of gaps in these programs, and assessment of whether these programs are sufficient to meet the needs of Federal, State, and local criminal justice personnel.

(4) Recommendations for opportunities, if any, to improve these programs in order to achieve greater efficiency, coherence, or effectiveness in the delivery of such training, education, and technical assistance, including through expansion, consolidation, or reorganization.

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

SEC. 4. CENTER OF EXCELLENCE FOR DIGITAL FORENSICS.

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

sultation with the Secretary of Homeland Security, shall designate an entity of the Federal Government as the Center of Excellence for Digital Forensics (hereafter, the ''Center'').

(b) MISSION.—The Center shall be a clearinghouse for training, technical expertise, and legal assistance relating to accessing digital evidence in support of criminal investigations, including by—

(1) serving as a central repository of knowledge and expertise regarding common types of data relevant to law enforcement investigations, common technical systems for storing and transmitting such data, formulation of lawful requests for such data, and procedures for submitting such requests;

(2) building and maintaining a library of analytic and forensic tools, along with technical expertise on the use of such tools, to be available to support Federal, State, and local law enforcement investigations;

(3) developing and maintaining technical support tools to facilitate, standardize, and authenticate law enforcement requests for digital evidence;

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

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

(5) producing and maintaining up-to-date training materials and curricula to support training of Federal, State, and local law enforcement organizations relating to digital evidence capacity by other training providers;

(6) coordinating with international, Federal, and State training programs, as well as relevant non-governmental stakeholders, to leverage and coordinate existing resources for training, technical assistance tools, and informative materials on procedures and techniques relating to digital evidence capacity; and

(7) providing a hotline available for law enforcement officials seeking advice about or assistance relating to digital evidence capacity.

(c) COORDINATION WITH EXISTING TRAINING PROVIDERS.—The designation required by subsection (a) shall be informed by the results of the review conducted under section 3.

(d) TERMINATION OR MODIFICATION OF DESIGNATION.—The Attorney General may terminate or modify

the designation under subsection (a) if the Attorney General, in consultation with the Secretary of Homeland Security, determines that the Center is no longer capable of achieving the missions specified in subsection (b) and designates a separate entity of the Federal Government to serve as the Center. Not later than 60 days before the effective date of such a termination, the Secretary shall provide written notice to Congress, including the rationale for such termination.

SEC. 5. FEDERAL GOVERNMENT LAW ENFORCEMENT TECHNOLOGY SUPPORT TO STATE AND LOCAL LAW ENFORCEMENT.

(a) PROGRAM.—The Attorney General and the Secretary of Homeland Security shall jointly establish a Law Enforcement Technology Support to State and Local Law Enforcement program under the direction of the Director of the Office of Digital Law Enforcement.

(b) DEVELOPMENT.—Under the program established in subsection (a), the Attorney General and the Secretary shall jointly develop guidelines and processes, as appropriate, to authorize the use of funds made available to grantees under the following programs for purposes of acquiring technology to improve the digital evidence capacity of law enforcement personnel:

(1) The Edward Byrne Memorial Justice Assistance Grant program.

(2) The Urban Area Security Initiative.

(3) The State Homeland Security Grant Program.

(c) DISSEMINATION OF ACQUISITION GUIDANCE.—Through the program established in subsection (a), the Attorney General and the Secretary shall develop guidance on acquisition of law enforcement technologies that support digital evidence capacity, and regularly disseminate such guidance to State and local law enforcement organizations. Such guidance shall identify and encourage adoption of effective law enforcement technologies useful across different technological platforms and formats.

(d) PUBLIC-PRIVATE PARTNERSHIPS.—Subject to the availability of resources, the Attorney General and the Secretary shall, under the program established in subsection (a), enter into partnerships with public or private entities to improve the access of Federal, State, and local law enforcement personnel to law enforcement technologies that support digital evidence capacity. Such partnerships may—

(1) develop collaborative approaches to developing new investigative tools;

(2) promote the exchange of technical experts between the technology and law enforcement communities;

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

(4) exchange information on technical approaches relating to digital evidence capacity, consistent with relevant laws and policies;

(5) develop training modules and content to support training of criminal justice personnel on relevant topics relating to digital evidence capacity; and

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

SEC. 6. DEPARTMENT OF JUSTICE TECHNOLOGY POLICY ADVISORY BOARD.

(a) ESTABLISHMENT.—There is established a Department of Justice Technology Policy Advisory Board (hereinafter in this section referred to as the ''Board''), which shall be composed of 11 members appointed in accordance with subsection (c) and shall conduct its business in accordance with this chapter.

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

(1) foster sustained dialogue between the technology and law enforcement communities on policy issues of mutual concern; and

(2) advise the Attorney General on—

(A) relevant developments in technologies relating to law enforcement, forensics, communications, and cybersecurity, and their implications for the Department of Justice;

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

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

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

(c) MEMBERS.—

(1) MEMBERS.—The members of the Board shall be senior non-government leaders with knowledge or expertise, whether by experience or training, in the fields of technology, communications, computer science, cybersecurity, digital forensics, law enforcement, relevant laws relating to digital searches and the use of digital evidence, and related fields, who shall be appointed by the Attorney General.

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

(3) VACANCIES.—Any vacancy in the membership of the Board shall not affect the powers of the Board and shall be filled in the same manner as the original appointment.

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

(d) COMPENSATION AND EXPENSES.—

(1) COMPENSATION.—A Member of the Board shall receive no compensation for the member's services as such.

(2) EXPENSES.—A member of the Board shall be allowed necessary travel expenses (or in the alternative, mileage for use of a privately owned vehicle and a per diem in lieu of subsistence not to exceed the rate and amount prescribed in sections 5702 and 5704 of title 5, United States Code), and other necessary expenses incurred by the member in the performance of duties vested in the Panel, without regard to the provisions of subchapter I of chapter 57 of title 5, United States Code, the Standardized Government Travel Regulations, or section 5731 of title 5, United States Code.

(e) SUPPORT.—The Attorney General shall provide support for the performance of the Board's functions and shall ensure compliance with the requirements of the Federal Advisory Committee Act of 1972 (5 U.S.C., Appendix), the Government in the Sunshine Act of 1976 (5 U.S.C. 552b), governing Federal statutes and regulations, and Department of Justice policies and procedures.

SEC. 7. DEFINITIONS.

For purposes of this Act:

(1) DIGITAL EVIDENCE CAPACITY.—The term ''digital evidence capacity'' shall include, in investigations and prosecutions involving digital evidence, the capacity, or activities supporting the capacity, to—

(A) acquire digital evidence in accordance with current surveillance, civil rights, and criminal justice laws;

(B) ensure digital evidence acquisition activities—

(i) minimize the acquisition of digital information not necessary to an investigation, including the acquisition of information pertaining to non-targeted persons;

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

court orders, and notice when required; and

(iii) favor less intrusive investigative techniques when they would suffice;

(C) handle and preserve digital evidence appropriately, including by ensuring—

(i) the integrity of the evidentiary chain of custody;

(ii) preventing inadvertent corruption or destruction of the evidence; and

(iii) promoting the prompt return of seized digital devices and the prompt return or destruction of seized digital information not used in prosecution of the crime for which it was acquired;

(D) extract, analyze, and exploit digital evidence;

(E) ensure the appropriate use of digital evidence, including by limiting the repurposing of seized digital information;

(F) use digital evidence in criminal legal proceedings; and

(G) ensure appropriate protections relating to privacy and security are applied to activities

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

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

○