The SPEAKER pro tempore announced the result of the vote as above recorded.

A motion to reconsider was laid on the table.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (Ms. ESSOEH) announced the following:

H.R. 2810, the National Defense Authorization Act of 2017, having been referred to the Committee on Armed Services, for consideration of sections 601, 701, 723, 727, 732, 3118, and 3119 of the House bill, and sections 601, 701, 725, 1089A, 1625, and 3114 of the Senate amendment, and modifications committed to conference: Messrs. TURNER, ROGERS of Alabama, FRANKS of California, Messrs. LANGEVIN, LARSEN of Maine, and Ms. SANGER of Washington, for consideration of section 1262 of the House bill, and sections 520A, 520B, and 3116 of the Senate amendment, and modifications committed to conference: Messrs. WALDEN, BARTON, and PALLONE of New Jersey.

H.R. 1616, the Strengthening State and Local Cyber Crime Fighting Act of 2017, having been referred to the Committee on the Judiciary, for consideration of sections 515, 1062, 1063, 1068, 1695, 2843, and 3117 of the House bill, and sections 520A, 520B, 520C, 520D, and 10804 of the Senate amendment, and modifications committed to conference: Messrs. BARR, WILLIAMS, and MAXINE of California, for consideration of section 701 of the Senate amendment, and modifications committed to conference: Messrs. ROYCE of California, DONOVAN, and ENGEL of New York.

H.R. 1616, the Strengthening State and Local Cyber Crime Fighting Act of 2017, having been referred to the Committee on the Judiciary, for consideration of sections 515, 1062, 1063, 1068, 1695, 2843, and 3117 of the House bill, and sections 520A, 520B, 520C, 520D, and 10804 of the Senate amendment, and modifications committed to conference: Messrs. ROYCE of California, DONOVAN, and ENGEL of New York.

The Clerk read the title of the bill.

The SPEAKER pro tempore. The Clerk will report the Senate amendment.

SEC. 2. AUTHORIZATION OF THE NATIONAL COMPUTER FORENSICS INSTITUTE OF THE DEPARTMENT OF HOMELAND SECURITY.

“(a) IN GENERAL.—Subtitle C of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 381 et seq.) is amended by adding at the end the following new section: “SEC. 822. NATIONAL COMPUTER FORENSICS INSTITUTE.”

“(b) FUNCTIONS.—The functions of the Institute shall include the following: “(1) Educating State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on current—
(A) cyber and electronic crimes and related threats;
(B) methods for investigating cyber and electronic crime and related threats and conducting computer and mobile device forensic examinations; and
(C) prosecutorial and judicial challenges related to cyber and electronic crime and related threats and conducting computer and mobile device forensic examinations.

(2) Training State, local, tribal, and territorial law enforcement officers to—
(A) conduct computer and mobile device forensic examinations; and
(B) respond to network intrusion incidents.

(3) Training State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on methods to obtain, process, store, and admit digital evidence in court.

(c) PRINCIPLES.—In carrying out the functions specified in subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and information related to cyber and electronic crime and related threats is shared among local, tribal, and territorial law enforcement officers and prosecutors.

(d) EQUIPMENT.—The Institute may provide State, local, tribal, and territorial law enforcement officers with computer equipment, hardware, software, manuals, and tools necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations.

(e) ELECTRONIC CRIME TASK FORCES.—The Institute shall facilitate the expansion of the network of Electronic Crime Task Forces of the United States Secret Service through the addition of State, local, tribal, and territorial law enforcement officers educated and trained at the Institute.

(f) SAVINGS PROVISION.—All authorized activities and functions carried out by the Institute at any location as of the day before the date of the enactment of this section are authorized to continue to be carried out at any such location on and after such date.

(b) FUNDING.—For each of fiscal years 2018 through 2022, amounts appropriated for the purposes of this title shall be used to support local efforts to identify, prevent, investigate, and prosecute cyber and financial crimes, including those crimes facilitated via computer networks and other electronic means, and crimes involving financial and economic impacts such as intellectual property crimes.

(c) GENERAL.—The funding for training to local, tribal, and territorial law enforcement officers, and other criminal justice professionals concerning the use of proven methodologies to prevent, detect, and respond to crimes, recognize emerging issues, manage electronic and financial crime evidence and to improve local criminal justice agency responses to such threats.

(d) TO PROVIDE OPERATIONAL AND TECHNICAL ASSISTANCE AND TRAINING CONCERNING TOOLS, PRODUCTS, RESOURCES, GUIDELINES, AND PROCEDURES TO AID IN THE INVESTIGATION AND LICIENT ANALYSIS, CONDUCT CYBER AND FINANCIAL CRIME INVESTIGATIONS, AND RELATED JUSTICE INFORMATION SHARING AT THE LOCAL AND STATE LEVELS.

(e) TO PROVIDE APPROPRIATE TRAINING ON PROTECTIONS FOR PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE CONDUCT OF CRIMINAL INTELLIGENCE ANALYSIS AND CYBER AND ELECTRONIC CRIME AND FINANCIAL CRIME INVESTIGATIONS, INCLUDING IN THE DEVELOPMENT OF POLICIES, GUIDELINES, AND PROCEDURES BY STATE, LOCAL, TRIBAL, AND TERRITORIAL LAW ENFORCEMENT AGENCIES TO PROTECT AND ENHANCE PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS AND IDENTIFY WEAKNESSES AND GAPS IN THE PROTECTION OF PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES.

(f) TO PROVIDE APPROPRIATE TRAINING ON PROTECTIONS FOR PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE CONDUCT OF CRIMINAL INTELLIGENCE ANALYSIS AND CYBER AND ELECTRONIC CRIME AND FINANCIAL CRIME INVESTIGATIONS, INCLUDING IN THE DEVELOPMENT OF POLICIES, GUIDELINES, AND PROCEDURES BY STATE, LOCAL, TRIBAL, AND TERRITORIAL LAW ENFORCEMENT AGENCIES TO PROTECT AND ENHANCE PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS AND IDENTIFY WEAKNESSES AND GAPS IN THE PROTECTION OF PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES.

SEC. 3033. AUTHORIZED PROGRAMS.

(A) Grant or cooperative agreement awarded under this title shall be made only for the following programs, with respect to the prevention, investigation, and prosecution of certain criminal activities:

(1) Programs to provide a nationwide support system for State and local criminal justice agencies.

(2) Programs to assist State and local criminal justice agencies to establish, develop, and maintain intelligence—focussed policing strategies and related information sharing.

(3) Programs to provide training and investigative support services to State and local criminal justice agencies to provide such services with resources and skills needed to investigate and prosecute such criminal activities and related criminal activities.

(4) Programs to provide research support, to establish partnerships, and to provide other resources to aid State and local criminal justice agencies to prevent, investigate, and prosecute such criminal activities and related problems.

(5) Programs to provide information and research to the general public to facilitate the prevention of such criminal activities.

(6) Programs to establish or support national training and research centers regionally to provide training and research services for State and local criminal justice agencies.

(b) WHITE COLLAR CRIME DEFINED.—For purposes of this part, the term ‘white collar crime’ includes—

(1) high-tech crime, including cyber and electronic crime and related threats;

(2) economic crime, including financial fraud and mortgage fraud; and

(3) Internet-based crime against children and child pornography.

SEC. 3032. PURPOSES.

The purposes of this part include the following:

(1) To ensure that training is available for State, local, tribal and territorial law enforcement agencies and officers nationwide to support local efforts to identify, prevent, investigate, and prosecute cyber and financial crimes, including those crimes facilitated via computer networks and other electronic means, and crimes involving financial and economic impacts such as intellectual property crimes.

(2) To ensure that training to local, tribal and territorial law enforcement officers, and other criminal justice professionals concerning the use of proven methodologies to prevent, detect and respond to crimes, recognize emerging issues, manage electronic and financial crime evidence and to improve local criminal justice agency responses to such threats.

(3) To provide operational and technical assistance and training concerning tools, products, resources, guidelines, and procedures to aid in the investigation and analysis, conduct cyber and financial crime investigations, and related justice information sharing at the local and State levels.

(4) To provide appropriate training on protections for privacy, civil rights, and civil liberties in the conduct of criminal intelligence analysis and cyber and electronic crime and financial crime investigations, including in the development of policies, guidelines, and procedures by State, local, tribal, and territorial law enforcement agencies to protect and enhance privacy, civil rights, and civil liberties protections and identify weaknesses and gaps in the protection of privacy, civil rights, and civil liberties.

(5) Programs to provide information and research to the general public to facilitate the prevention of such criminal activities.