H. R. 4651

To establish in the legislative branch the National Commission on Security and Technology Challenges.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 29, 2016

Mr. McCaul (for himself, Mr. Langevin, Mr. Meehan, Ms. DelBene, Mr. Bishop of Michigan, Mr. Ted Lieu of California, Mr. Hurd of Texas, Miss Rice of New York, Mr. Párethold, Mr. Swalwell of California, Mr. Donovan, Mr. McNearney, Mrs. Comstock, Mrs. Mimi Walters of California, Mr. Costello of Pennsylvania, and Mr. Reichert) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committees on the Judiciary and Foreign Affairs, 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 in the legislative branch the National Commission on Security and Technology Challenges.

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

2. SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

3. (a) Short Title.—This Act may be cited as the “Digital Security Commission Act of 2016”.


(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Findings.
Sec. 3. Establishment of the National Commission on Security and Technology Challenges.
Sec. 4. Composition of Commission.
Sec. 5. Reports to Congress.
Sec. 6. Powers of Commission.
Sec. 7. Nonapplicability of Federal Advisory Committee Act.
Sec. 8. Staff.
Sec. 9. Meeting and hearings.
Sec. 10. Termination.
Sec. 11. Funding.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Today, more than ever before, digital security and communications technology, national security, public safety, and counterterrorism are inextricably linked; indeed, digital security and communications technology plays a critically important role in efforts to keep the United States and its citizens safe.

(2) Technological innovation and development is critical to the United States economy and the competitiveness of United States businesses in the global marketplace.

(3) Technology companies represent some of the largest employers in the United States and contribute significantly to the gross domestic product of the United States.
(4) The digital security and communications technology that the people of the United States use every day to protect communications and data, including encryption, is essential to the present and future of the United States.

(5) Digital security and communications technology helps to protect critical infrastructure, financial and banking systems, health records, online security, commercial transactions, proprietary enterprise and governmental information, and privacy and civil liberties.

(6) The same technology that benefits the people of the United States in so many ways also presents new challenges; in the wrong hands, digital security and communications technology can be used to facilitate crime and terrorism and is used by malicious actors, including drug traffickers, child predators, and cybercriminals, to carry out criminal activities.

(7) Terrorist and criminal organizations use digital security and communications technology to evade law enforcement and national security entities when plotting attacks and recruiting supporters in the United States and abroad, and law enforcement and national security authorities have indicated that
the use of this technology presents unique challenges to their ability to protect the public.

(8) Rapidly evolving technological advancements drive the modern economy in many ways, but can also create challenges for the law enforcement and national security communities.

(9) Ensuring that analysts, law enforcement officers, and policymakers fully understand the dynamic digital landscape will become increasingly important in the coming decades.

(10) The United States currently faces the difficult question of how best to take advantage of the security and privacy benefits digital security and communications technology provides, while at the same time ensuring that the dangers posed by the use of digital security and communications technology by terrorists and criminals is mitigated; indeed, the challenge is to reconcile equally important security interests.

(11) Despite years of dialogue between the technology sector, law enforcement, national security professionals, and others, no clear path forward has been developed that would benefit each of the critical security interests simultaneously; rather, there seems to be a consensus among stakeholders, lawmakers,
and experts that the question of reconciling competing security interests is one without an easy or obvious answer.

(12) Leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community, global commerce and economics, and the national security community must be brought together to examine these issues in a systematic, holistic way and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.

(13) It is important to approach these issues with recognition that the communications marketplace is increasingly global and marked by competition from foreign firms and the growing prominence of international technical standards.

(14) With respect to competing security interests, it is incumbent upon the United States to be forward-thinking and to assess how it can and should adapt to the emerging challenges of the digital world.
SEC. 3. ESTABLISHMENT OF THE NATIONAL COMMISSION ON SECURITY AND TECHNOLOGY CHALLENGES.

(a) IN GENERAL.—There is established in the legislative branch a commission to be known as the “National Commission on Security and Technology Challenges” (in this Act referred to as the “Commission”).

(b) PURPOSES.—The purposes of the Commission are the following:

(1) To bring together leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community, global commerce and economies, and the national security community to examine the intersection of security and digital security and communications technology in a systematic, holistic way, and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.

(2) To submit to Congress a report, which shall include, at a minimum, each of the following:

(A) An assessment of the issue of multiple security interests in the digital world, including public safety, privacy, national security, and
communications and data protection, both now
and throughout the next 10 years.

(B) A qualitative and quantitative assess-
ment of—

(i) the economic and commercial value
of cryptography and digital security and
communications technology to the economy
of the United States;

(ii) the benefits of cryptography and
digital security and communications tech-
nology to national security and crime pre-
vention;

(iii) the role of cryptography and dig-
ital security and communications tech-
nology in protecting the privacy and civil
liberties of the people of the United States;

(iv) the effects of the use of cryptog-
raphy and other digital security and com-
munications technology on Federal, State,
and local criminal investigations and
counterterrorism enterprises;

(v) the costs of weakening cryptog-
raphy and digital security and communica-
tions technology standards; and
(vi) international laws, standards, and practices regarding legal access to communications and data protected by cryptography and digital security and communications technology, and the potential effect the development of disparate, and potentially conflicting, laws, standards, and practices might have.

(C) Recommendations for policy and practice, including, if the Commission determines appropriate, recommendations for legislative changes, regarding—

(i) methods to be used to allow the United States Government and civil society to take advantage of the benefits of digital security and communications technology while at the same time ensuring that the danger posed by the abuse of digital security and communications technology by terrorists and criminals is sufficiently mitigated;

(ii) the tools, training, and resources that could be used by law enforcement and national security agencies to adapt to the new realities of the digital landscape;
(iii) approaches to cooperation between the Government and the private sector to make it difficult for terrorists to use digital security and communications technology to mobilize, facilitate, and operationalize attacks;

(iv) any revisions to the law applicable to wiretaps and warrants for digital data content necessary to better correspond with present and future innovations in communications and data security, while preserving privacy and market competitiveness;

(v) proposed changes to the procedures for obtaining and executing warrants to make such procedures more efficient and cost-effective for the Government, technology companies, and telecommunications and broadband service providers; and

(vi) any steps the United States could take to lead the development of international standards for requesting and obtaining digital evidence for criminal investigations and prosecutions from a foreign,
sovereign State, including reforming the mutual legal assistance treaty process, while protecting civil liberties and due process.

SEC. 4. COMPOSITION OF COMMISSION.

(a) Members.—The Commission shall be composed of 16 members, as follows:

(1) Eight members who shall be appointed by the Speaker of the House and the Senate majority leader, one from each of the fields specified in subsection (b). One such member shall serve as the chairman of the Commission.

(2) Eight members who shall be appointed by the minority leader in the House and the minority leader in the Senate, one from each of the fields specified in subsection (b). One such member shall serve as the vice chairman of the Commission.

(3) One additional individual who shall be appointed by the President and who shall serve in an ex officio capacity as a nonvoting member.

(b) Qualifications.—In accordance with subsection (a), individuals appointed to the Commission shall be United States citizens with significant knowledge and primary experience relevant to the mission of the Commission in one of the following fields:
(1) Cryptography.

(2) Global commerce and economics.

(3) Federal law enforcement.

(4) State and local law enforcement.

(5) Consumer-facing technology sector.

(6) Enterprise technology sector.

(7) The intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))).

(8) The privacy and civil liberties community.

(c) DEADLINE FOR APPOINTMENT.—All members of the Commission, with the exception of those serving in an ex officio capacity, shall be appointed by not later than 30 days after the date of the enactment of this Act.

(d) VACANCIES.—Any vacancy in the Commission shall not affect its powers, but shall be filled in the same manner in which the original appointment was made.

(e) COMPENSATION.—While away from their homes or regular places of business in the performance of services for the Commission, members of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.

(f) MEETINGS; RULES OF PROCEDURE; QUORUM.—
(1) MEETINGS.—The Commission shall hold its initial meeting and begin the operations of the Commission by not later than 60 days after the date of the enactment of this Act. After such initial meeting, the Commission shall meet upon the call of the chairman or a majority of its members.

(2) QUORUM.—A simple majority of members of the Commission shall constitute a quorum.

(3) VOTING.—No proxy voting shall be allowed on behalf of a member of the Commission.

(4) RULES OF PROCEDURE.—The Commission may establish rules for the conduct of the Commission’s business, if such rules are not inconsistent with this Act or other applicable laws.

(5) NOTICE.—The chairman of the Commission shall provide 5 business days advance notice for any meeting or hearing of the Commission.

(g) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall cooperate with the Commission in expeditiously providing appropriate security clearances to Commission members, as may be requested, to the extent possible pursuant to existing procedures and requirements, except that no person shall be provided with access to classified information without the appropriate security clearances.
SEC. 5. REPORTS TO CONGRESS.

(a) INTERIM REPORTS.—Not later than six months after its initial meeting, the Commission shall submit to the Speaker of the House of Representatives, the Senate majority leader, the House of Representatives minority leader, the Senate minority leader, the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on the Judiciary of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, the Committee on Energy and Commerce of the House of Representatives, and the Committee on Commerce, Science, and Transportation of the Senate a report outlining the activities of the Commission to date, a plan of action moving forward, and any initial findings, that have been agreed to by at least 12 of the 16 voting members. Thereafter, the Commission may submit to the congressional entities named above any additional interim reports that have been agreed to by at least 12 of the 16 members of the Commission.

(b) FINAL REPORT.—Not later than 12 months after the date of the initial meeting of the Commission, the Commission shall submit to the congressional entities listed in subsection (a) a final report containing such find-
ings, conclusions, and recommendations as have been
greed to by at least 12 of the 16 voting members of the
Commission.

(c) DISSENTING VIEWS.—The Rules of Procedure es-
established in section 4(f)(4) of this Act shall include proce-
dures by which any minority of commissioners may issue
dissenting views, including dissenting findings and rec-
ommendations.

(d) FORM.—Reports required under this paragraph
shall be submitted in unclassified form but may include
a classified annex.

SEC. 6. POWERS OF COMMISSION.

(a) HEARINGS AND INFORMATION.—The Commission
may, for the purpose of carrying out this Act—

(1) hold such hearings and sit and act at such
times and places, take such testimony, receive such
information, and administer such oaths as the Com-
misson or such designated subcommittee or des-
ignated member may determine advisable; and

(2) subject to paragraph (1), require, by sub-
poena or otherwise, the attendance and testimony of
such witnesses and the production of such books,
records, correspondence, memoranda, papers, and
documents, as the Commission or such designated
subcommittee or designated member may determine advisable.

(b) Subpoenas.—

(1) Issuance.—

(A) In general.—A subpoena for information that is materially relevant to the duties of the Commission may be issued under this subsection only by the affirmative vote of at least 12 of the 16 voting members of the Commission.

(B) Signature.—Subject to subparagraph (A), subpoenas issued under this subsection may be issued under the signature of the chairman, and may be served by any person designated by the chairman or by a member designated by a majority of the Commission.

(2) Enforcement.—In the case of contumacy or failure to obey a subpoena issued under paragraph (1), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found, or where the subpoena is returnable, may issue an order requiring such person to appear at any designated place to testify or to produce documentary or other evidence.
Any failure to obey the order of the court may be punished by the court as contempt of that court.

(c) CONTRACTING.—The Commission may, to such extent and in such amounts as are provided in appropriation Acts, enter into contracts to enable the Commission to discharge its duties under this Act.

(d) INFORMATION FROM FEDERAL AGENCIES.—The Commission is authorized to secure directly from any executive department, bureau, agency, board, commission, office, independent establishment, or instrumentality of the Government, information, suggestions, estimates, and statistics for the purposes of this Act. The head of each such department, bureau, agency, board, commission, office, independent establishment, or instrumentality shall, to the extent authorized by law, furnish such information, suggestions, estimates, and statistics directly to the Commission, upon request made by the chairman and vice chairman, the chairman of any subcommittee created by a majority of the Commission, or any member designated by a majority of the Commission.

(e) RECEIPT, HANDLING, AND STORAGE OF INFORMATION.—Sensitive or proprietary information shall only be received, handled, and stored by members of the Commission and its staff consistent with all applicable statutes, regulations, and Executive orders.
(f) DISSEMINATION OF INFORMATION.—Information obtained by members and staff of the Commission may not be revealed or disseminated outside of the Commission absent approval from a majority of the members of the Commission. In addition, any dissemination of information must be consistent with all applicable statutes, regulations, and Executive orders.

(g) ASSISTANCE FROM FEDERAL AGENCIES.—

(1) GENERAL SERVICES ADMINISTRATION.—
Upon request by the executive director of the Commission, the Administrator of General Services shall provide to the Commission on a reimbursable basis administrative support and other services for the performance of the Commission’s functions under this Act.

(2) OTHER DEPARTMENTS AND AGENCIES.—In addition to the assistance prescribed in paragraph (1), the heads of Federal departments and agencies may provide to the Commission such services, funds, facilities, staff, and other support services as such heads may determine advisable and as may be authorized by law.

(h) POSTAL SERVICES.—The Commission may use the United States mail in the same manner and under the
same conditions as departments and agencies of the United States.

SEC. 7. NONAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.

The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission.

SEC. 8. STAFF.

(a) APPOINTMENT.—The chairman and vice chairman shall jointly appoint and fix the compensation of an executive director and of and such other personnel as may be necessary to enable the Commission to carry out its functions under this Act.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall cooperate with the Commission in expeditiously providing appropriate security clearances to Commission staff, as may be requested, to the extent possible pursuant to existing procedures and requirements, except that no person shall be provided with access to classified information without the appropriate security clearances.

(c) DETAILLEES.—Any Federal Government employee may be detailed to the Commission on a reimbursable basis, and such detailee shall retain without interruption the rights, status, and privileges of his or her regular employment.
(d) Expert and Consultant Services.—The Commission is authorized to procure the services of experts and consultants in accordance with section 3109 of title 5, United States Code, but at rates not to exceed the daily rate paid a person occupying a position level IV of the Executive Schedule under section 5315 of title 5, United States Code.

(e) Volunteer Services.—Notwithstanding section 1342 of title 31, United States Code, the Commission may accept and use voluntary and uncompensated services as the Commission determines necessary.

SEC. 9. MEETING AND HEARINGS.

(a) Public Meetings and Release of Public Versions of Reports.—The Commission shall—

(1) hold public hearings and meetings to the extent appropriate; and

(2) release public versions of the reports required under section 5.

(b) Public Hearings.—Any public hearings of the Commission shall be conducted in a manner consistent with the protection of information provided to, or developed for or by the Commission, as required by any applicable statute, regulation, or Executive order.

(c) Private Hearings.—Any private hearings of the Commission shall be conducted in a manner consistent
with the protection of information provided to, or developed for or by the Commission, as required by any applicable statute, regulation, or Executive order. To the extent practicable, the Commission shall release summaries of any official private hearings.

SEC. 10. TERMINATION.

(a) IN GENERAL.—The Commission, and all the authorities of this Act, shall terminate on the date that is 60 days after the date on which the final report is submitted under section 5(b).

(b) ADMINISTRATIVE ACTIVITIES BEFORE TERMINATION.—The Commission may use the 60-day period referred to in subsection (a) for the purpose of concluding its activities, including providing testimony to committees of Congress concerning its reports and disseminating the final report under section 5(b).

SEC. 11. FUNDING.

(a) AUTHORIZATION OF APPROPRIATION.—No additional funds are authorized to be appropriated to carry out this Act.

(b) DURATION OF AVAILABILITY.—Amounts made available to the Commission under subsection (a) are authorized to remain available until the termination of the Commission in accordance with section 10.
(c) REMAINING FUNDS.—Any funds remaining upon termination of the Commission under section 10 shall be returned to the general fund of the Treasury for the purpose of deficit reduction.