115TH CONGRESS
1ST SESSION

S. _____

To establish a voluntary program to identify and promote Internet-connected products that meet industry-leading cybersecurity and data security standards, guidelines, best practices, methodologies, procedures, and processes.

IN THE SENATE OF THE UNITED STATES

Mr. MARKEY introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish a voluntary program to identify and promote Internet-connected products that meet industry-leading cybersecurity and data security standards, guidelines, best practices, methodologies, procedures, and processes.

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 ''Cyber Shield Act of 2017''.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''Advisory Committee'' means the Cyber Shield Advisory Committee established under section 3(a);

(2) the term ''benchmarks'' means standards, guidelines, best practices, methodologies, procedures, and processes;

(3) the term ''covered product'' means a consumer-facing physical object that can—

(A) connect to the Internet; and

(B) collect, send, or receive data;

(4) the term ''Cyber Shield program'' means the voluntary program established under section 4(a)(1); and

(5) the term ''Secretary'' means the Secretary of Commerce.

SEC. 3. CYBER SHIELD ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—Not later than 90 days after the date of enactment of this Act, the Secretary shall establish a Cyber Shield Advisory Committee.

(b) DUTIES.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Advisory Committee shall provide recommendations to the Secretary regarding—

(A) the format and content of the Cyber Shield labels required to be established under section 4; and

(B) the process for identifying, establishing, reporting on, adopting, maintaining, and promoting compliance with the voluntary cybersecurity and data security benchmarks required to be established under section 4.

(2) PUBLIC AVAILABILITY OF RECOMMENDATIONS.—The Advisory Committee shall publish, and provide the public with an opportunity to comment on, the recommendations provided to the Secretary under paragraph (1).

(c) MEMBERS, CHAIRMAN, AND DUTIES.—

(1) APPOINTMENT.—

(A) IN GENERAL.—The Advisory Committee shall be composed of members appointed by the Secretary from among individuals who are specially qualified to serve on the Advisory Committee based on their education, training, or experience.

(B) REPRESENTATION.—Members appointed under subparagraph (A) shall include—

(i) representatives of the covered products industry, including small, medium, and large businesses;

(ii) cybersecurity experts;

(iii) public interest advocates; and

(iv) Federal employees with expertise in certification, covered devices, or cybersecurity, including employees of the Department of Commerce, the Federal Trade Commission, and the Federal Communications Commission.

(C) LIMITATION.—In appointing members under subparagraph (A), the Secretary shall ensure that—

(i) each interest group described in clauses (i) through (iv) of subparagraph (B) is proportionally represented on the Advisory Committee, including—

(I) businesses of each size described in such clause (i);

(II) Federal employees with expertise in each subject described in such clause (iv); and

(III) Federal employees from each agency described in such clause (iv); and

(ii) no single interest group is represented by a majority of the members of the Advisory Committee.

(2) CHAIR.—The Secretary shall designate a member of the Advisory Committee to serve as Chair.

(3) PAY.—Members of the Advisory Committee shall serve without pay, except that the Secretary may allow a member, while attending meetings of the Advisory Committee or a subcommittee of the Advisory Committee, expenses authorized under section 5703 of title 5, United States Code, relating to per diem, travel, and transportation.

(d) SUPPORT STAFF; ADMINISTRATIVE SERVICES.—

(1) SUPPORT STAFF.—The Secretary shall provide support staff for the Advisory Committee.

(2) ADMINISTRATIVE SERVICES.—Upon request by the Advisory Committee, the Secretary shall provide any information, administrative services, and supplies that the Secretary considers necessary for the Advisory Committee to carry out its duties and powers.

(e) NO TERMINATION.—Section 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Advisory Committee.

SEC. 4. CYBER SHIELD PROGRAM.

(a) ESTABLISHMENT OF PROGRAM.—

(1) IN GENERAL.—The Secretary shall establish a voluntary program to identify and certify covered products with superior cybersecurity and data security through voluntary certification and labeling of, and other forms of communication about, covered products and subsets of covered products that meet industry-leading cybersecurity and data security benchmarks to enhance cybersecurity and protect data.

(2) GRADES.—Labels applied to products under the Cyber Shield program—

(A) may be digital; and

(B) may be in the form of different grades that display the extent to which a product meets the industry-leading cybersecurity and data security benchmarks.

(b) CONSULTATION.—Not later than 90 days after the date of enactment of this Act, the Secretary shall establish a process for consulting interested parties, the Secretary of Health and Human Services, the Commissioner

of Food and Drugs, the Secretary of Homeland Security, and other Federal agencies in carrying out the Cyber Shield program.

(c) DUTIES.—In carrying out the Cyber Shield program, the Secretary—

(1) shall—

(A) establish and maintain cybersecurity and data security benchmarks, by convening and consulting interested parties and other Federal agencies, for products with the Cyber Shield label to ensure that those products perform better than their less secure counterparts; and

(B) in carrying out subparagraph (A)—

(i) engage in an open public review and comment process;

(ii) in consultation with the Advisory Committee, identify and apply cybersecurity and data security benchmarks to different subsets of covered products based on—

(I) cybersecurity and data security risk;

(II) the sensitivity of the information collected, transmitted, or stored by the product; and

(III) product functionality; and

(iii) to the extent possible, incorporate existing benchmarks when establishing and maintaining cybersecurity and data security benchmarks;

(2) may not establish benchmarks under paragraph (1) that are—

(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; or

(B) unsupported by evidence;

(3) shall permit a manufacturer or distributor of a covered product to display a Cyber Shield label reflecting the extent to which the product meets the industry-leading cybersecurity and data security benchmarks established under paragraph (1);

(4) shall promote technologies that are compliant with the cybersecurity and data security benchmarks established by the Secretary as the preferred technologies in the marketplace for—

(A) enhancing cybersecurity; and

(B) protecting data;

(5) shall work to enhance public awareness of the Cyber Shield label, including through public outreach, education, research and development, and other means;

(6) shall preserve the integrity of the Cyber Shield label;

(7) if helpful in fulfilling the obligation under paragraph (6), may elect to not treat a covered product as a Cyber Shield-certified product until the product meets appropriate conformity standards, which may include—

(A) testing by an accredited third-party certifying laboratory or other entity in accordance with the Cyber Shield program; and

(B) certification by the laboratory or entity described in subparagraph (A) as meeting the applicable cybersecurity and data security benchmarks established by the Secretary;

(8) not less frequently than once every 2 years after establishing cybersecurity and data security benchmarks for a product category under paragraph (1), shall review and, if appropriate, update the cybersecurity and data security benchmarks for that product category;

(9) shall solicit comments from interested parties and the Advisory Committee prior to establishing or revising a Cyber Shield product category or benchmark (or prior to the effective date of the establishment or revision of a product category or benchmark);

(10) upon adoption of a new or revised product category or benchmark, shall provide reasonable notice to interested parties of any changes (including effective dates) to product categories or benchmarks, along with—

(A) an explanation of the changes; and

(B) as appropriate, responses to comments submitted by interested parties; and

(11) shall provide appropriate lead time prior to the applicable effective date for a new or a significant revision to a product category or benchmark, taking into account the timing requirements of the manufacturing, product marketing, and distribution process for the product or products addressed.

(d) DEADLINES.—Not later than 2 years after the date of enactment of this Act, the Secretary shall establish cybersecurity and data security benchmarks for covered products under subsection (c)(1), which shall take effect

not later than 60 days after the date on which the benchmarks are established.

(e) ADMINISTRATION.—The Secretary, in consultation with the Advisory Committee, may enter into a contract with a third party to administer the Cyber Shield program if—

(1) the third party is an impartial administrator; and

(2) entering into the contract improves the cybersecurity and data security of covered products.

(f) PROGRAM EVALUATION.—

(1) IN GENERAL.—Not later than 4 years after the date of enactment of this Act, and not less frequently than every 2 years thereafter, the Inspector General of the Department of Commerce shall evaluate the Cyber Shield program.

(2) REQUIREMENTS.—In conducting an evaluation under paragraph (1), the Inspector General of the Department of Commerce shall—

(A) evaluate the extent to which the cybersecurity and data security benchmarks established under the Cyber Shield program address cybersecurity and data security threats;

(B) assess how the benchmarks have evolved to meet emerging cybersecurity and data security threats;

(C) conduct covert testing to evaluate the integrity of certification testing; and

(D) assess the costs to businesses of participating in the Cyber Shield program.

SEC. 5. CYBER SHIELD DIGITAL PRODUCT PORTAL.

(a) IN GENERAL.—The Secretary shall make publicly available on the website of the Department of Commerce in a searchable format—

(1) a web page providing information about the Cyber Shield program; and

(2) a database of covered products certified under the Cyber Shield program.

(b) REQUIREMENTS.—The database established under subsection (a) shall include—

(1) the cybersecurity and data security benchmarks for each product category; and

(2) for each covered product certified under the Cyber Shield program—

(A) the certification for the product;

(B) the name and manufacturer of the product;

(C) the contact information for the manufacturer;

(D) the functionality of the product;

(E) the location of any applicable privacy policy; and

(F) any other information the Secretary determines necessary and appropriate.

SEC. 6. RULE OF CONSTRUCTION.

The decision of a manufacturer of a covered product not to participate in the Cyber Shield program shall not affect the liability of the manufacturer for a cybersecurity or data security breach of that covered product.