116TH 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, and for other purposes.

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, 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 ''Cyber Shield Act of 2019''.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''Advisory Committee'' means the Cyber Shield Advisory Committee established by the Secretary 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 or other network; and

(B)(i) collect, send, or receive data; or

(ii) control the actions of a physical object or system;

(4) the term ''Cyber Shield program'' means the voluntary program established by the Secretary 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 the 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, CHAIR, 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 the education, training, or experience of those individuals.

(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, including independent cybersecurity researchers that specialize in areas such as cryptanalysis, hardware and software security, wireless and network security, cloud security, and data privacy;

(iii) public interest advocates;

(iv) a liaison from the Information Security and Privacy Advisory Board established under section 21(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(a)) who is a member of that Board as described in paragraph (3) of such section 21(a);

(v) Federal employees with expertise in certification, covered devices, or cybersecurity, including employees of—

(I) the Department of Commerce;

(II) the National Institute of Standards and Technology;

(III) the Federal Trade Commission;

(IV) the Federal Communications Commission; and

(V) the Consumer Product Safety Commission; and

(vi) an expert who shall ensure that, subject to subsection (e), the Advisory Committee conforms to and complies with the requirements under the Federal Advisory Committee Act (5 U.S.C. App.).

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

(i) each interest group described in clauses (i), (ii), (iii), and (v) of subparagraph (B) is proportionally represented on the Advisory Committee, including—

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

(II) Federal employees with expertise in each subject described in clause (v) of that subparagraph; and

(III) Federal employees from each agency described in subclauses

(I) through (V) of clause (v) of that subparagraph; and

(ii) no single interest group described in clauses (i), (ii), (iii), and (v) of subparagraph (B) 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, per diem, travel, and transportation expenses authorized under section 5703 of title 5, United States Code.

(d) SUPPORT STAFF; ADMINISTRATIVE SERVICES.—

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

(2) ADMINISTRATIVE SERVICES.—Upon the request of 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 the duties and powers of the Advisory Committee.

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

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this section.

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 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) LABELS.—Labels applied to covered products under the Cyber Shield program—

(A) shall be digital and, if feasible, physical and affixed to the covered product or packaging; and

(B) may be in the form of different grades that display the extent to which a covered 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 the heads of other Federal agencies in carrying out the Cyber Shield program.

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

(1) shall—

(A) by convening and consulting interested parties and the heads of other Federal agencies, establish and maintain cybersecurity and data security benchmarks for covered products with the Cyber Shield label to ensure that those covered products perform better than counterparts of those covered products that do not have the Cyber Shield label; 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 dif-

ferent subsets of covered products based on, with respect to each such subset—

(I) any cybersecurity and data security risk relating to covered products in the subset;

(II) the sensitivity of the information collected, transmitted, or stored by covered products in the subset;

(III) the functionality of covered products in the subset;

(IV) the security practices and testing procedures used in developing and manufacturing covered products in the subset;

(V) the level of expertise, qualifications, and professional accreditation of the staff employed by the manufacturers of covered products in the subset who are responsible for cybersecurity of the covered products; and

(VI) any other criteria the Advisory Committee and Secretary determine is necessary and appropriate; and

(iii) to the extent possible, incorporate existing cybersecurity and data security benchmarks, such as the baseline of cybersecurity features defined in the document entitled ''Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers'', published by the National Institute of Standards and Technology in July 2019, or any successor thereto;

(2) may not establish any cybersecurity and data security benchmark under paragraph (1) that is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

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

(4) shall promote technologies, practices, and policies that—

(A) are compliant with the cybersecurity and data security benchmarks established under paragraph (1); and

(B) the Secretary determines are the preferred technologies, practices, and policies in the marketplace for—

(i) enhancing cybersecurity;

(ii) ensuring that cybersecurity is incorporated in all aspects of the life cycle of a covered product; and

(iii) 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 covered product certified under the Cyber Shield program until the covered product meets appropriate conformity standards, which may include—

(A) standards relating to 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) that the covered product meets the applicable cybersecurity and data security benchmarks established under paragraph (1);

(8) not less frequently than annually after the date on which the Secretary establishes cybersecurity and data security benchmarks for a covered product category under paragraph (1), shall review, and, if appropriate, update the cybersecurity and data security benchmarks, for that covered product category;

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

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

(A) an explanation of the changes; and

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

(11) shall provide appropriate lead time before the applicable effective date for a new or a significant revision to a covered product category or cybersecurity and data security benchmark, taking into account the timing requirements of the manufacturing, marketing, and distribution process for any covered product addressed; and

(12) may remove the certification of a covered product as a covered product certified under the Cyber Shield program if the manufacturer of the certified covered product falls out of conformity with the benchmarks established under paragraph (1) for the covered product, as determined by the Secretary.

(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 Secretary establishes the cybersecurity and data security benchmarks.

(e) ADMINISTRATION.—The Secretary, in consultation with the Advisory Committee, may enter into a con-

tract 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 3 years after the date on which the Secretary establishes cybersecurity and data security benchmarks for covered products under subsection (c)(1), and not less frequently than every 3 years thereafter, the Inspector General of the Department of Commerce shall—

(A) evaluate the Cyber Shield program; and

(B) submit a report on the results of the evaluation carried out under subparagraph (A) to—

(i) the Committee on Commerce, Science, and Transportation of the Senate; and

(ii) the Committee on Energy and Commerce of the House of Representatives.

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

(A) with respect to the cybersecurity and data security benchmarks established under subsection (c)(1)—

(i) evaluate the extent to which the cybersecurity and data security benchmarks address cybersecurity and data security threats; and

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

(B) conduct covert testing of covered products to evaluate the integrity of certification testing under the Cyber Shield program;

(C) assess the costs to businesses that manufacture covered products of participating in the Cyber Shield program;

(D) evaluate the level of participation in the Cyber Shield program by businesses that manufacture covered products;

(E) assess the level of public awareness and consumer awareness of the Cyber Shield label;

(F) determine whether any private sector or international cybersecurity certification programs comparable to the Cyber Shield program exist; and

(G) if any private sector or international cybersecurity certification programs described in subparagraph (F) exist, evaluate how each such private sector or international cybersecurity certification program interacts with and compares to the Cyber Shield program.

(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this section.

SEC. 5. CYBER SHIELD DIGITAL COVERED 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;

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

(3) contact information for each manufacturer of a covered product certified under the Cyber Shield program that may be used by consumers to contact the manufacturer regarding questions or complaints.

(b) REQUIREMENTS.—The database established under subsection (a)(2) shall include—

(1) the cybersecurity and data security benchmarks established under section 4(c)(1) for each covered product category; and

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

(A) the certification for the covered product;

(B) the name and manufacturer of the covered product;

(C) the contact information for the manufacturer of the covered product;

(D) the functionality of the covered product;

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

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

SEC. 6. RULE OF CONSTRUCTION.

The decision of a manufacturer of a covered product to not 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.