

115TH CONGRESS
1ST SESSION

S. 1656

To amend the Federal Food, Drug, and Cosmetic Act to provide cybersecurity protections for medical devices.

IN THE SENATE OF THE UNITED STATES

JULY 27, 2017

Mr. BLUMENTHAL introduced the following bill; which was read twice and referred to the Committee on Health, Education, Labor, and Pensions

A BILL

To amend the Federal Food, Drug, and Cosmetic Act to provide cybersecurity protections for medical devices.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Medical Device Cyber-
5 security Act of 2017”.

6 **SEC. 2. CYBERSECURITY FOR MEDICAL DEVICES.**

7 (a) IN GENERAL.—Chapter V of the Federal Food,
8 Drug, and Cosmetic Act (21 U.S.C. 351 et seq.) is amend-
9 ed by inserting after section 520 (21 U.S.C. 360j) the fol-
10 lowing—

1 **“SEC. 520A. CYBERSECURITY FOR DEVICES.**

2 “(a) DEFINITIONS.—In this section:

3 “(1) CYBER DEVICE.—The term ‘cyber device’
4 means any device that has network or Internet
5 connectivity (such as near field communication
6 (NFC), Bluetooth, or WiFi), connects to an external
7 storage device or external media (such as a universal
8 serial bus (USB) or a compact disk), or has any
9 other cyber capability.

10 “(2) CYBERSECURITY FIX OR UPDATE.—The
11 term ‘cybersecurity fix or update’ means any modi-
12 fication to a cyber device that addresses a software,
13 firmware, or hardware error or known vulnerability,
14 or a security update, and does not change the thera-
15 peutic or diagnostic function of the device.

16 “(b) TRANSPARENCY OF RISK PRIOR TO MAR-
17 KETING.—

18 “(1) REPORT CARD.—

19 “(A) IN GENERAL.—The Secretary, in co-
20 ordination with the entities described in sub-
21 paragraph (B), shall develop a report card for
22 indicating the cybersecurity functions of cyber
23 devices. The report card shall contain the con-
24 tents described in paragraph (2) and be dis-
25 closed in accordance with paragraph (3).

1 “(B) COORDINATION.—The entities de-
2 scribed in this subparagraph are the following:

3 “(i) The National Institute of Stand-
4 ards and Technology.

5 “(ii) The Secretary of Homeland Se-
6 curity.

7 “(iii) The National Coordination Of-
8 fice supporting the Networking and Infor-
9 mation Technology Research and Develop-
10 ment Program.

11 “(iv) The Federal Trade Commission.

12 “(v) Any other relevant agency, or cy-
13 bersecurity or medical device industry
14 group, as determined by the Secretary.

15 “(2) CONTENTS OF REPORT CARD.—Each re-
16 port card shall contain each of the following:

17 “(A) Information pertaining to all essential
18 elements described in the most recent version of
19 the Manufacturer Disclosure Statement for
20 Medical Device Security, as set forth by the
21 Healthcare Information and Management Sys-
22 tems Society and the National Electrical Manu-
23 facturers Association.

24 “(B) A traceability matrix, accepted by the
25 Secretary, that—

1 “(i) redacts content that is confiden-
2 tial, as determined by the Secretary; and

3 “(ii) establishes design components
4 and traces such components to design com-
5 pensating controls.

6 “(C) A description of any manufacturer
7 compensating controls that—

8 “(i) effectively address known com-
9 mon vulnerabilities and exposures; and

10 “(ii) provide providers with industry
11 standard compensating controls for im-
12 proving cybersecurity.

13 “(D) A description of—

14 “(i) any cybersecurity evaluation con-
15 ducted on the device, including any testing,
16 validation, or verification of the device;

17 “(ii) who conducted such evaluation;
18 and

19 “(iii) the results of such evaluation.

20 “(E) A cybersecurity risk assessment con-
21 ducted by the manufacturer, or a third party,
22 explaining the risk of the device to patient safe-
23 ty and clinical hazards.

24 “(F) An indication of whether the device is
25 capable of being remotely accessed. If the device

1 is capable of being remotely accessed, an indica-
2 tion of any security measures and access proto-
3 cols the device has in place to secure such ac-
4 cess.

5 “(3) DISCLOSURE OF REPORT CARD.—

6 “(A) CLEARANCE OR APPROVAL.—The
7 manufacturer of any cyber device shall include
8 the report card in any notification to the Sec-
9 retary under section 510(k) or any application
10 for premarket approval under section 515(c), as
11 applicable.

12 “(B) PUBLIC ACCESSIBILITY.—

13 “(i) IN GENERAL.—The Secretary
14 shall provide a copy of the report card to
15 any entity described in clause (ii) that sub-
16 mits a request for such copy to the Sec-
17 retary.

18 “(ii) ENTITIES PERMITTED ACCESS.—

19 An entity described in this clause is—

20 “(I) any health care industry en-
21 tity, consisting of any provider, device
22 manufacturer, the Federal Govern-
23 ment, health care information security
24 researchers, and health care aca-
25 demia; and

1 “(II) any entity determined by
2 the Secretary to have a valid interest
3 in the report card.

4 “(C) UPDATED REPORT CARD.—For as
5 long as the cyber device receives technical sup-
6 port from the manufacturer or any other third
7 party authorized by the manufacturer, the man-
8 ufacturer shall submit to the Secretary an an-
9 nual update to the report card.

10 “(c) PROTECTING REMOTE ACCESS TO MANAGED
11 SOLUTIONS.—

12 “(1) IN GENERAL.—A manufacturer of a cyber
13 device shall:

14 “(A) In order to remotely access such de-
15 vice after selling, or otherwise transferring own-
16 ership of, the device, obtain consent for such
17 access from the provider owning or operating
18 the device and from any patient on which the
19 device is used. Such consent may be in the form
20 of an agreement entered into between the pro-
21 vider and the manufacturer at the time the de-
22 vice is sold to the provider, and may be for the
23 manufacturer to remotely access the device at
24 times specified in such agreement or by an
25 agreement between the manufacturer and pro-

1 vider entered into thereafter. In the case of an
2 agreement described in the previous sentence,
3 consent of the patient may be obtained through
4 the provider notifying the patient of such agree-
5 ment.

6 “(B) For any cyber device that the manu-
7 facturer may remotely access in accordance
8 with subparagraph (A):

9 “(i) Notify the provider when the
10 manufacturer accesses the device remotely,
11 including the name of the person with such
12 access, the kinds of tasks that can be per-
13 formed through such access, and the soft-
14 ware used to access the device. Such notifi-
15 cation can be in the form of an audit log
16 described in clause (ii) if the audit log is
17 readily available to the provider.

18 “(ii) Maintain an audit log for each
19 time the manufacturer accesses the device
20 remotely and make such log accessible to
21 the provider.

22 “(C) Except as provided in paragraph (2),
23 for any cyber device that has the capability to
24 be accessed remotely by the manufacturer or
25 any other entity:

1 “(i) Implement multi-factor authentication for accessing any cyber capability
2 of the device.
3

4 “(ii) Secure data in motion and data
5 at rest with data encryption, and other
6 best practices, approved by the National
7 Institute of Standards and Technology.

8 “(iii) Install automated tools to track
9 access, or identify attempts at unauthorized
10 access, to any cyber capability of the
11 device.

12 “(iv) Adopt whitelisting approaches
13 and changeable passwords for accessing
14 any cyber capability of the device.

15 “(v) Comply with the remote access
16 provisions recommended by the National
17 Institute of Standards and Technology, in
18 the document entitled ‘Security for Tele-
19 commuting and Broadband Communica-
20 tions (NIST Special Publication 800–46)’,
21 published in August 2002.

22 “(2) EXCEPTIONS.—A manufacturer may submit
23 a petition to the Secretary to exempt a cyber de-
24 vice from any requirement under paragraph (1)(C).
25 The Secretary may grant such an exemption if it de-

1 termines that the manufacturer can prove the ex-
2 emption would pose not more than a minimal risk to
3 patient health, minimal risk to privacy, and minimal
4 risk of a cyber vulnerability.

5 “(d) CYBERSECURITY FIXES OR UPDATES.—

6 “(1) RE-CLEARANCE OR REAPPROVAL.—Unless
7 at the request of the Secretary due to a unique and
8 extenuating circumstance, any cybersecurity fix or
9 update shall not require a new notification under
10 section 510(k) or application for premarket approval
11 under section 515(c).

12 “(2) FREE CYBERSECURITY FIXES OR UP-
13 DATES.—A manufacturer of a cyber device shall pro-
14 vide any cybersecurity fix or update to the device
15 free of charge until—

16 “(A) the date on which any agreement to
17 provide such fixes or updates, entered into be-
18 tween the manufacturer (or a third party au-
19 thorized by the manufacturer) and a provider,
20 expires; or

21 “(B) if no agreement described in subpara-
22 graph (A) is in effect, the date that is 10 years
23 after the date on which the manufacturer dis-
24 continues marketing the device.

1 “(e) END-OF-LIFE DEVICE.—Not later than 90 days
2 after a manufacturer declares that it will no longer sell
3 a cyber device, the manufacturer of such device shall—

4 “(1) shall provide any provider owning or oper-
5 ating the device with the report card, as most re-
6 cently updated under subsection (b)(3)(C);

7 “(2) to the extent practicable, inform any pro-
8 vider owning or operating the device that the manu-
9 facturer will no longer be manufacturing such de-
10 vice;

11 “(3) provide notice to any provider owning or
12 operating the device of the date on which the last cy-
13 bersecurity fix or update will be provided by the
14 manufacturer;

15 “(4) notify the Secretary of such declaration;
16 and

17 “(5) provide any provider owning or operating
18 the device with the following information related to
19 the device:

20 “(A) Compensating controls on how to se-
21 curely configure the cyber device if the device
22 stays in operation past the date on which the
23 manufacturer stops providing cybsecurity fixes
24 or updates under subsection (d)(2).

1 “(B) Documentation on secure preparation
2 for recycling and disposal of the device.

3 “(C) Specific guidance regarding sup-
4 porting infrastructure architecture, including
5 network segmentation and device isolation re-
6 quirements.

7 “(D) Instructions on how to delete any
8 personally identifiable information, protected
9 health information, or other site-specific sen-
10 sitive data such as configuration files.

11 “(f) APPLICABILITY.—This section shall not apply
12 with respect to any cyber device for which, prior to the
13 enactment of the Medical Device Cybersecurity Act of
14 2017, a notification was submitted under section 510(k),
15 or for which an application for premarket approval was
16 submitted under section 515(c).”.

17 (b) ENFORCEMENT.—Section 301 of the Federal
18 Food, Drug, and Cosmetic Act (21 U.S.C. 331) is amend-
19 ed by adding at the end the following:

20 “(eee) The failure to comply with subsection (b), (c),
21 (d), or (e) of section 520A.”.

22 (c) EXPANSION OF ICS–CERT RESPONSIBILITIES.—

23 (1) DEFINITIONS.—In this subsection:

24 (A) CYBER DEVICE.—The term “cyber de-
25 vice” has the meaning given the term in section

1 520A of the Federal Food, Drug, and Cosmetic
2 Act, as added by subsection (a).

3 (B) ICS–CERT.—The term “ICS–CERT”
4 means the Industrial Control Systems Cyber
5 Emergency Response Team of the National Cy-
6 bersecurity and Communications Integration
7 Center established under section 227 of the
8 Homeland Security Act of 2002 (6 U.S.C. 148).

9 (C) UNDER SECRETARY.—The term
10 “Under Secretary” means the Under Secretary
11 appointed under section 103(a)(1)(H) of the
12 Homeland Security Act of 2002 (6 U.S.C.
13 113(a)(1)(H)).

14 (2) EXPANSION.—Not later than 180 days after
15 the date of enactment of this Act, the Under Sec-
16 retary shall expand the duties and mission of ICS–
17 CERT to include—

18 (A) investigating cybersecurity vulnerabili-
19 ties of cyber devices that may cause harm to
20 human life or significant misuse of personal
21 health information, as determined necessary by
22 ICS–CERT or at the request of the Under Sec-
23 retary; and

1 (B) coordinating device-specific responses
2 to cybersecurity incidents and vulnerabilities
3 with respect to cyber devices.

4 (3) CONSULTATION.—In carrying out para-
5 graph (2), the Under Secretary shall consult with
6 relevant agencies within the Food and Drug Admin-
7 istration, the Department of Health and Human
8 Services, the National Institute of Standards and
9 Technology, the National Coordination Office for
10 Networking and Information Technology Research
11 and Development, the Federal Trade Commission,
12 and experts in the cybersecurity and medical device
13 industries.

14 (4) COORDINATED DISCLOSURE.—Not later
15 than 6 months after the date of enactment of this
16 Act, the Secretary of Homeland Security shall issue
17 rules relating to the coordinated disclosure of con-
18 trolled and uncontrolled cybersecurity vulnerabilities
19 of cyber devices, which shall—

20 (A) outline the roles and responsibilities of
21 ICS–CERT and manufacturers and providers of
22 cyber devices;

23 (B) provide timelines for all required ac-
24 tions; and

1 (C) provide for the enforcement of coopera-
2 tion between ICS-CERT and manufacturers
3 and providers of cyber devices.

4 (5) REPORT.—Not later than 1 year after the
5 date of enactment of this Act, the Under Secretary
6 shall submit to Congress a report detailing the ex-
7 panded duties and mission of ICS-CERT under
8 paragraph (2).

○