II

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.

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 ''Medical Device Cybersecurity Act of 2017''.

SEC. 2. CYBERSECURITY FOR MEDICAL DEVICES.

(a) IN GENERAL.—Chapter V of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 351 et seq.) is amended by inserting after section 520 (21 U.S.C. 360j) the following—

"SEC. 520A. CYBERSECURITY FOR DEVICES.

"(a) DEFINITIONS.—In this section:

"(1) CYBER DEVICE.—The term 'cyber device' means any device that has network or Internet connectivity (such as near field communication (NFC), Bluetooth, or WiFi), connects to an external storage device or external media (such as a universal serial bus (USB) or a compact disk), or has any other cyber capability.

"(2) CYBERSECURITY FIX OR UPDATE.—The term 'cybersecurity fix or update' means any modification to a cyber device that addresses a software, firmware, or hardware error or known vulnerability, or a security update, and does not change the therapeutic or diagnostic function of the device.

"(b) TRANSPARENCY OF RISK PRIOR TO MARKETING.—

"(1) REPORT CARD.—

"(A) IN GENERAL.—The Secretary, in coordination with the entities described in subparagraph (B), shall develop a report card for indicating the cybersecurity functions of cyber devices. The report card shall contain the contents described in paragraph (2) and be disclosed in accordance with paragraph (3).

''(B) COORDINATION.—The entities described in this subparagraph are the following:

''(i) The National Institute of Standards and Technology.

''(ii) The Secretary of Homeland Security.

''(iii) The National Coordination Office supporting the Networking and Information Technology Research and Development Program.

''(iv) The Federal Trade Commission.

''(v) Any other relevant agency, or cybersecurity or medical device industry group, as determined by the Secretary.

''(2) CONTENTS OF REPORT CARD.—Each report card shall contain each of the following:

''(A) Information pertaining to all essential elements described in the most recent version of the Manufacturer Disclosure Statement for Medical Device Security, as set forth by the Healthcare Information and Management Systems Society and the National Electrical Manufacturers Association.

''(B) A traceability matrix, accepted by the Secretary, that—

"(i) redacts content that is confidential, as determined by the Secretary; and

"(ii) establishes design components and traces such components to design compensating controls.

"(C) A description of any manufacturer compensating controls that—

"(i) effectively address known common vulnerabilities and exposures; and

"(ii) provide providers with industry standard compensating controls for improving cybersecurity.

"(D) A description of—

"(i) any cybersecurity evaluation conducted on the device, including any testing, validation, or verification of the device;

"(ii) who conducted such evaluation; and

"(iii) the results of such evaluation.

"(E) A cybersecurity risk assessment conducted by the manufacturer, or a third party, explaining the risk of the device to patient safety and clinical hazards.

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

is capable of being remotely accessed, an indication of any security measures and access protocols the device has in place to secure such access.

''(3) DISCLOSURE OF REPORT CARD.—

''(A) CLEARANCE OR APPROVAL.—The manufacturer of any cyber device shall include the report card in any notification to the Secretary under section 510(k) or any application for premarket approval under section 515(c), as applicable.

''(B) PUBLIC ACCESSIBILITY.—

''(i) IN GENERAL.—The Secretary shall provide a copy of the report card to any entity described in clause (ii) that submits a request for such copy to the Secretary.

''(ii) ENTITIES PERMITTED ACCESS.—An entity described in this clause is—

''(I) any health care industry entity, consisting of any provider, device manufacturer, the Federal Government, health care information security researchers, and health care academia; and

"(II) any entity determined by the Secretary to have a valid interest in the report card.

"(C) UPDATED REPORT CARD.—For as long as the cyber device receives technical support from the manufacturer or any other third party authorized by the manufacturer, the manufacturer shall submit to the Secretary an annual update to the report card.

"(c) PROTECTING REMOTE ACCESS TO MANAGED SOLUTIONS.—

"(1) IN GENERAL.—A manufacturer of a cyber device shall:

"(A) In order to remotely access such device after selling, or otherwise transferring ownership of, the device, obtain consent for such access from the provider owning or operating the device and from any patient on which the device is used. Such consent may be in the form of an agreement entered into between the provider and the manufacturer at the time the device is sold to the provider, and may be for the manufacturer to remotely access the device at times specified in such agreement or by an agreement between the manufacturer and pro-

vider entered into thereafter. In the case of an agreement described in the previous sentence, consent of the patient may be obtained through the provider notifying the patient of such agreement.

''(B) For any cyber device that the manufacturer may remotely access in accordance with subparagraph (A):

''(i) Notify the provider when the manufacturer accesses the device remotely, including the name of the person with such access, the kinds of tasks that can be performed through such access, and the software used to access the device. Such notification can be in the form of an audit log described in clause (ii) if the audit log is readily available to the provider.

''(ii) Maintain an audit log for each time the manufacturer accesses the device remotely and make such log accessible to the provider.

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

''(i) Implement multi-factor authentication for accessing any cyber capability of the device.

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

''(iii) Install automated tools to track access, or identify attempts at unauthorized access, to any cyber capability of the device.

''(iv) Adopt whitelisting approaches and changeable passwords for accessing any cyber capability of the device.

''(v) Comply with the remote access provisions recommended by the National Institute of Standards and Technology, in the document entitled 'Security for Telecommuting and Broadband Communications (NIST Special Publication 800–46)', published in August 2002.

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

termines that the manufacturer can prove the exemption would pose not more than a minimal risk to patient health, minimal risk to privacy, and minimal risk of a cyber vulnerability.

''(d) CYBERSECURITY FIXES OR UPDATES.—

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

''(2) FREE CYBERSECURITY FIXES OR UPDATES.—A manufacturer of a cyber device shall provide any cybersecurity fix or update to the device free of charge until—

''(A) the date on which any agreement to provide such fixes or updates, entered into between the manufacturer (or a third party authorized by the manufacturer) and a provider, expires; or

''(B) if no agreement described in subparagraph (A) is in effect, the date that is 10 years after the date on which the manufacturer discontinues marketing the device.

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

''(1) shall provide any provider owning or operating the device with the report card, as most recently updated under subsection (b)(3)(C);

''(2) to the extent practicable, inform any provider owning or operating the device that the manufacturer will no longer be manufacturing such device;

''(3) provide notice to any provider owning or operating the device of the date on which the last cybersecurity fix or update will be provided by the manufacturer;

''(4) notify the Secretary of such declaration; and

''(5) provide any provider owning or operating the device with the following information related to the device:

''(A) Compensating controls on how to securely configure the cyber device if the device stays in operation past the date on which the manufacturer stops providing cybsecurity fixes or updates under subsection (d)(2).

''(B) Documentation on secure preparation for recycling and disposal of the device.

''(C) Specific guidance regarding supporting infrastructure architecture, including network segmentation and device isolation requirements.

''(D) Instructions on how to delete any personally identifiable information, protected health information, or other site-specific sensitive data such as configuration files.

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

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

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

(c) EXPANSION OF ICS–CERT RESPONSIBILITIES.—

(1) DEFINITIONS.—In this subsection:

(A) CYBER DEVICE.—The term ''cyber device'' has the meaning given the term in section

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

(B) ICS–CERT.—The term ''ICS–CERT'' means the Industrial Control Systems Cyber Emergency Response Team of the National Cybersecurity and Communications Integration Center established under section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148).

(C) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary appointed under section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H)).

(2) EXPANSION.—Not later than 180 days after the date of enactment of this Act, the Under Secretary shall expand the duties and mission of ICS–CERT to include—

(A) investigating cybersecurity vulnerabilities of cyber devices that may cause harm to human life or significant misuse of personal health information, as determined necessary by ICS–CERT or at the request of the Under Secretary; and

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

(3) CONSULTATION.—In carrying out paragraph (2), the Under Secretary shall consult with relevant agencies within the Food and Drug Administration, the Department of Health and Human Services, the National Institute of Standards and Technology, the National Coordination Office for Networking and Information Technology Research and Development, the Federal Trade Commission, and experts in the cybersecurity and medical device industries.

(4) COORDINATED DISCLOSURE.—Not later than 6 months after the date of enactment of this Act, the Secretary of Homeland Security shall issue rules relating to the coordinated disclosure of controlled and uncontrolled cybersecurity vulnerabilities of cyber devices, which shall—

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

(B) provide timelines for all required actions; and

(C) provide for the enforcement of cooperation between ICS–CERT and manufacturers and providers of cyber devices.

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

○