119TH CONGRESS
2D SESSION

S. _____

To require the Secretary of Health and Human Services to review certain medical devices manufactured in the People's Republic of China for potential cybersecurity issues, and for other purposes.

IN THE SENATE OF THE UNITED STATES

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

A BILL

To require the Secretary of Health and Human Services to review certain medical devices manufactured in the People's Republic of China for potential cybersecurity issues, 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 ''Countering Chinese Cyberthreats for Patients Act'' or the ''Countering CCP Act''.

SEC. 2. REVIEW AND RECALL OF CERTAIN MEDICAL DEVICES MANUFACTURED IN THE PEOPLE'S REPUBLIC OF CHINA.

(a) REVIEW OF CERTAIN DEVICES.—

(1) IN GENERAL.—The Secretary of Health and Human Services, acting through the Commissioner of Food and Drugs (referred to in this section as the ''Secretary''), in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall review each covered device for potential cybersecurity issues.

(2) REQUEST FOR INFORMATION.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall request from each covered manufacturer of a covered device such information as is necessary to conduct the review under paragraph (1), including—

(i) a software bill of materials for the covered device, including commercial, open-source, and off-the-shelf software components, and data mapping and architecture documentation;

(ii) locations of entities, information systems, and servers holding patient data; and

(iii) any other information the Secretary determines necessary.

(B) REQUIREMENTS.—In determining the form and scope of information to request under subparagraph (A), the Secretary, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall analyze covered devices and seek information, including information on any processes and procedures of the covered manufacturer, that, as determined by Secretary, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency—

(i) would provide a reasonable assurance that the covered device and related systems are and will remain cybersecure; and

(ii) would provide a reasonable assurance that patient data would not be stored or transferred through systems or servers located in, owned, or controlled by entities

headquartered or subject to jurisdiction of the People's Republic of China.

(b) RECALL AUTHORITY.—

(1) IN GENERAL.—Subject to paragraph (3), not later than 18 months after the date of enactment of this Act, the Secretary shall issue for all covered devices that are determined pursuant to the review under subsection (a) to pose a cybersecurity risk an order requiring the appropriate person (including the manufacturers, importers, distributors, or retailers of the covered device)—

(A) to immediately cease distribution of such covered device;

(B) to immediately notify health professionals and device user facilities of the order and to instruct such professionals and facilities to cease use of such covered device; and

(C) to notify all individuals subject to the risks associated with the use of such covered device.

(2) RECALL IN CASES OF FAILURE TO PROVIDE INFORMATION.—Subject to paragraph (3), for any covered device for which the covered manufacturer fails to submit the information requested under subsection (a)(2)(A) by the date that is 180 days after

the date on which such covered manufacturer received such request, the Secretary shall issue for such covered device an order requiring the appropriate person (including the manufacturers, importers, distributors, or retailers of the covered device)—

(A) to immediately cease distribution of such covered device;

(B) to immediately notify health professionals and device user facilities of the order and to instruct such professionals and facilities to cease use of such covered device; and

(C) to notify all individuals subject to the risks associated with the use of such covered device.

(3) EXEMPTION.—The Secretary may exempt from an order under paragraph (1) or (2) a covered device for which a recall would, as determined by the Secretary, create a shortage that would pose a danger to patient health.

(c) REPORT.—Not later than 2 years after the date of enactment of this Act, the Secretary, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall submit to the Committee on Health, Education, Labor and Pensions and the Committee on Homeland Security and Governmental Affairs

of the Senate and the Committee on Energy and Commerce and the Committee on Homeland Security of the House of Representatives a report that includes—

(1) a description of the cyber preparedness and data security of the device industry in the United States;

(2) an analysis of the market share of devices used in the United States of manufacturers headquartered in the People's Republic of China;

(3) an analysis of data security requirements and protections of devices used in the United States of manufacturers headquartered in or subject to the jurisdiction of the People's Republic of China; and

(4) recommendations for methods to bolster the cyber preparedness of the device industry in the United States.

(d) DEFINITIONS.—In this section:

(1) COVERED DEVICE.—The term ''covered device'' means a networked device that was manufactured by a covered manufacturer and was cleared, authorized, approved, or exempted under section 510(k), 513(f)(2), 515, or 520(m) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 360(k), 360c(f)(2), 360e, 360j(m)) on or before March 28, 2023.

(2) COVERED MANUFACTURER.—

(A) IN GENERAL.—The term ''covered manufacturer'' means a manufacturer—

(i) headquartered in the People's Republic of China; or

(ii) that is owned or controlled by—

(I) the People's Republic of China; or

(II) 1 or more individuals or entities of the People's Republic of China.

(B) EXCLUSION.—The term ''covered manufacturer'' does not include a manufacturer that has operations, subsidiaries, or publicly traded securities in the People's Republic of China if such manufacturer is not otherwise a manufacturer described in subparagraph (A).

(3) CYBERSECURITY RISK.—The term ''cybersecurity risk'' means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism.

(4) NETWORKED.—The term ''networked'', with respect to a device, means that the device includes software that has the ability to connect to the internet.