Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act

---

Guidance for Industry and Food and Drug Administration Staff

Document issued on March 30, 2023.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

FDA U.S. FOOD & DRUG ADMINISTRATION

Preface

Public Comment

You may submit electronic comments and suggestions at any time for Agency consideration to https://www.regulations.gov. Submit written comments to the Dockets Management Staff, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852. Identify all comments with the docket number FDA-2023-D-1030. Comments may not be acted upon by the Agency until the document is next revised or updated.

Additional Copies

CDRH

Additional copies are available from the Internet. You may also send an email request to CDRH-Guidance@fda.hhs.gov to receive a copy of the guidance. Please include the document number GUI00007021 and complete title of the guidance in the request.

CBER

Additional copies are available from the Center for Biologics Evaluation and Research (CBER), Office of Communication, Outreach, and Development (OCOD), 10903 New Hampshire Ave., WO71, Room 3128, Silver Spring, MD 20903, or by calling 1-800-835-4709 or 240-402-8010, by email, ocod@fda.hhs.gov, or from the Internet at https://www.fda.gov/vaccines-blood-biologics/guidance-compliance-regulatory-information-biologics/biologics-guidances.

Table of Contents

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices Under Section 524B of the FD&C Act

---

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

I. Introduction

On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus — "Ensuring Cybersecurity of Medical Devices" — amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices. The Omnibus states that the amendments to the FD&C Act shall take effect 90 days after the enactment of this Act on March 29, 2023. As provided by the Omnibus, the cybersecurity requirements do not apply to an application or submission submitted to the Food and Drug Administration (FDA) before March 29, 2023.

This guidance is being implemented without prior public comment because FDA has determined that prior public participation for this guidance is not feasible or appropriate (see section 701(h)(1)(C) of the FD&C Act (21 U.S.C. 371(h)(1)(C)) and 21 CFR 10.115(g)(2)). This guidance document is being implemented immediately, but it remains subject to comment in accordance with the Agency's good guidance practices.

In general, FDA's guidance documents do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word should in Agency guidances means that something is suggested or recommended, but not required.

II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

> (a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).
>
> (b) The sponsor of an application or submission described in subsection (a) shall-
>
> (1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;
>
> (2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address—
>
> (A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and
>
> (B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;
>
> (3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and
>
> (4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.
>
> (c) DEFINITION.—In this section, the term 'cyber device' means a device that—
>
> (1) includes software validated, installed, or authorized by the sponsor as a device or in a device;
>
> (2) has the ability to connect to the internet; and
>
> (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance

documents, Refuse to Accept Policy for 510(k)s,[1] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[2] and Acceptance Review for De Novo Classification Requests.[3]

[1] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/refuse-accept-policy-510ks.
[2] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/acceptance-and-filing-reviews-premarket-approval-applications-pmas.
[3] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/acceptance-review-de-novo-classification-requests.