Contains Nonbinding Recommendations

Draft – Not for Implementation

Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act

---

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on March 13, 2024.

You should submit comments and suggestions regarding this draft document within 60 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments 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 20852-1740. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions about this document regarding CDRH-regulated devices, contact CDRHManufacturerShortage@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.

When final, this guidance will supersede "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," issued September 27, 2023.

U.S. FOOD & DRUG ADMINISTRATION

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

Preface

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 GUI00001825 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., Bldg. 71, Room 3128, Silver Spring, MD 20993-0002, 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.

Contains Nonbinding Recommendations

Draft – Not for Implementation

Table of Contents

Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act

Draft Guidance for Industry and Food and Drug Administration Staff

This draft guidance, when finalized, will represent 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. Overview of Select Updates

The Food and Drug Administration (FDA or Agency) has developed this draft guidance to propose select updates to the FDA guidance "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" (hereafter referred to as the "Premarket Cybersecurity Guidance").[1] The Premarket Cybersecurity Guidance, in its current form, remains the Agency's current thinking on this topic until this draft guidance is finalized, at which time the finalized version of Section II. of this draft guidance will be added as Section VII. of the Premarket Cybersecurity Guidance. FDA intends to incorporate the updates proposed in this draft guidance into the Premarket Cybersecurity Guidance as one final guidance document after obtaining and considering public comment on these proposed select updates. The sections of the existing Premarket Cybersecurity Guidance that are unaffected by these proposed updates are not intended to be substantively changed, with the exception of technical edits for consistency.

Section 3305 of the Food and Drug Omnibus Reform Act of 2022 ("FDORA"), enacted on December 29, 2022, added section 524B "Ensuring Cybersecurity of Medical Devices" to the FD&C Act. Under section 524B(a) of the FD&C Act, a person who submits a 510(k), Premarket Approval Application (PMA), Product Development Protocol (PDP), De Novo, or Humanitarian Device Exemption (HDE) submission for a device that meets the definition of a "cyber device," as defined under section 524B(c) of the FD&C Act, is required to submit information to ensure that cyber devices meet the cybersecurity requirements under section 524B(b) of the FD&C Act.

[1] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

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. Cyber Devices

FDA is proposing to add a Section VII. to the Premarket Cybersecurity Guidance with the following language in this Section II. This section identifies the cybersecurity information FDA considers to generally be necessary to support obligations under section 524B of the FD&C Act.

A. Who is Required to Comply with Section 524B of the FD&C Act

Under section 524B(a) of the FD&C Act, a person, including a manufacturer,[2] who submits a premarket application or submission under any of the following pathways 510(k),[3] PMA,[4] PDP, De Novo, or HDE[5] for a device that meets the definition of a "cyber device," as defined in section 524B(c) of the FD&C Act, is required to include such information as FDA may require to ensure that the cyber device meets the cybersecurity requirements under section 524B(b) of the FD&C Act.

B. Devices Subject to Section 524B of the FD&C Act

Section 524B of the FD&C Act and its requirements apply to "cyber devices." Section 524B(c) of the FD&C Act defines a "cyber device" as 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."

Informed in part by the definitions recognized by the National Institute for Standards and Technology (NIST) for the term "software," FDA considers a "cyber device" to include devices

[2] Section 524B(a) of the FD&C Act places obligations on the "person" who submits a specific type of device marketing application. Section 524B(b) of the FD&C Act places obligations on a "sponsor." For the purposes of this guidance, we assume that the manufacturer is the entity submitting the application and use the term accordingly throughout the guidance in lieu of the term "person" or "sponsor." However, if another person submits the application or submission enumerated under section 524B(a) of the FD&C Act to the Agency, that person should follow the guidance for manufacturers herein. Whatever person submits the application for a cyber device is subject to the requirements of section 524B.

[3] For the purposes of this guidance "510(k)" refers to the original, special, and abbreviated 510(k) applications.

[4] For the purposes of this guidance "PMA" refers to the original PMA and supplement PMAs.

[5] For the purposes of this guidance "HDE" refers to the original HDE and supplement HDEs.

that are or contain software, including software that is firmware or programmable logic.[6] FDA also considers the "ability to connect to the internet" to include devices that are able to connect to the internet, whether intentionally or unintentionally, through any means (including at any point identified in the evaluation of the threat surface[7] of the device and the environment of use). It is well-demonstrated that if a device has the ability to connect to the Internet, it is possible that it can be connected to the Internet, regardless of whether such connectivity was intended by the device sponsor.[8]

FDA considers devices that include any of the following features to have the ability to connect to the internet. The list below is illustrative, not exhaustive:

- Wi-Fi or cellular;
- Network, server, or Cloud Service Provider connections;
- Bluetooth or Bluetooth Low Energy;
- Radiofrequency communications;
- Inductive communications; and
- Hardware connectors capable of connecting to the internet (e.g., USB, ethernet, serial port).

C. Documentation Recommendations to Comply with 524B

For applicable premarket submission types, manufacturers must provide documentation to comply with the requirements under section 524B of the FD&C Act. Recommendations regarding the documentation to support each of the requirements is discussed in the sections below.

[6] NIST defines a programmable logic controller (PLC) as "[a] solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing." A PLC is therefore a combination of two components: (1) the hardware controller, and (2) the "user-programmable memory," or programmable logic, that instructs the hardware controller to execute specified functions. NIST defines software as, among other things, "computer programs and data stored in hardware – typically in read only memory or programmable read-only memory." Programmable logic is therefore a specific type of computer program and/or data stored on hardware, and is thus a type of software. *See* https://csrc.nist.gov/glossary for more information on NIST's definitions of these terms.

[7] For the purposes of this guidance, "threat surface" means the set of points on the boundary of a system, a system element, or an environment where a cyber threat can try to enter, cause an effect on, or extract data from, that system, system element, or environment" (definition is adapted from https://csrc.nist.gov/glossary/). For the purposes of this guidance "threat surface" is synonymous with the term "attack surface," however, FDA uses the term "threat surface" rather than "attack surface," because cyber threats need not necessarily be an "attack" to pose a risk to a medical device and its related system.

[8] *See* https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf; https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/?sh=43561087425c

1. Plans and Procedures (Section 524B(b)(1))

Section 524B(b)(1) of the FD&C Act requires manufacturers of cyber devices to submit to FDA "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" in their premarket submissions. We recommend that the plan contain the information recommended for the Cybersecurity Management Plan described in Section VI.B. of the Premarket Cybersecurity Guidance. Additionally, such a plan should also address the additional items discussed below.

First, FDA considers that coordinated vulnerability disclosure (CVD) and related procedures could include:

- Coordinated disclosure of vulnerabilities and exploits identified by external entities (including third-party software suppliers and researchers);
- Disclosure of vulnerabilities and exploits identified by the manufacturer of cyber devices; and
- Manufacturer procedures to carry out disclosures of the vulnerabilities and exploits, as identified above.[9]

Second, plans required by section 524B(b)(1) of the FD&C Act should also describe the timeline, with associated justifications, to develop and release required updates and patches:

- Section 524B(b)(2)(A) of the FD&C Act requires manufacturers of cyber devices to make updates and patches for known unacceptable vulnerabilities available on a reasonably justified regular cycle.
- Section 524B(b)(2)(B) of the FD&C Act requires manufacturers of cyber devices to make available updates and patches to the device and related systems[10] to address as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks.

Third, we recommend that manufacturers of cyber devices anticipate and make appropriate updates to these plans,[11] as well as to the processes, and procedures discussed in section II.C.2. below,[12] as new information becomes available, such as when new risks, threats, vulnerabilities, assets, or adverse impacts are discovered throughout the total product lifecycle. To support such efforts, manufacturers should also create or update appropriate documentation (e.g., threat modeling) and maintain it throughout the device lifecycle. Doing so will allow manufacturers to quickly identify vulnerability impacts once a device is released and could also help satisfy the patching requirements of section 524B(b)(2)(A)-(B) of the FD&C Act.

---

[9] For the purposes of this guidance, manufacturer procedures to carry out disclosures of the vulnerabilities and exploits may include procedures to inform device users, customers, patients, and other relevant healthcare stakeholders.

[10] For the purposes of this guidance, we are considering "related systems" to the extent needed to determine that the device, as it interacts with related systems, remains cybersecure. Related systems are further described in Section II.C.2, below.

[11] *See* section 524B(b)(1) of the FD&C Act.

[12] *See* section 524B(b)(2) of the FD&C Act.

The required plans,[13] as well as the processes, and procedures discussed in section II.C.2. below,[14] also should, as appropriate, account for any differences in the risk management for fielded devices (e.g., differences between marketed devices and devices no longer marketed but still in use). For example, if an update is not applied automatically for all fielded devices, then there will likely be different risk profiles for the differing software configurations of the device. Vulnerabilities should be assessed for any differing impacts for all fielded versions to ensure patient risks are being accurately assessed.

2. Design, Develop, and Maintain Processes and Procedures to Provide a Reasonable Assurance of Cybersecurity (Section 524B(b)(2))

Manufacturers of cyber devices must "design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure . . ." (section 524B(b)(2) of the FD&C Act). FDA considers related systems to include, among other things, manufacturer-controlled elements, such as other devices, software that performs "other functions" as described in FDA's Guidance "Multiple Function Device Products: Policy and Considerations,"[15] software/firmware update servers, and connections to health care facility networks. The documentation recommendations identified in the Premarket Cybersecurity Guidance and summarized in Appendix 4 of the same guidance should be considered and used to demonstrate reasonable assurance that the device and related systems are cybersecure as required by section 524B(b)(2) of the FD&C Act.

3. Software Bill of Materials (SBOM) (Section 524B(b)(3))

Section 524B(b)(3) of the FD&C Act requires manufacturers of cyber devices to provide an SBOM, including commercial, open-source, and off-the-shelf software components. To assist with complying with this requirement, we recommend that a cyber device provide SBOMs that contain the information recommended in Section V.A.4(b) of the Premarket Cybersecurity Guidance.

D. Modifications

The new requirements under section 524B of the FD&C Act apply to a person who submits an application or submission under section 510(k), 513(De Novo), 515(c)(PMA), 515(f)(PDP) or 520(m)(HDE) for a device that meets the definition of a cyber device. Therefore, a person required to submit an application under one of the enumerated provisions for a device modification would also need to comply with the requirements in section 524B of the FD&C

[13] *See* section 524B(b)(1) of the FD&C Act.
[14] *See* section 524B(b)(2) of the FD&C Act.
[15] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/multiple-function-device-products-policy-and-considerations

Act. In keeping with least burdensome principles,[16] the information we recommend that manufacturers of cyber devices provide will generally differ based on the type of change and whether such change impacts the cybersecurity of the device. Overall, we recommend that manufacturers use the recommendations below to determine the information FDA recommends manufacturers of cyber devices provide to demonstrate they have met the new requirements under section 524B of the FD&C Act when submitting a premarket submission for a device modification.

1. Changes That May Impact Cybersecurity

In general, changes that may impact cybersecurity could include changes to authentication or encryption algorithms, new connectivity features, or changing software update process/mechanisms. For these types of changes, see Section II.C., above, for required and recommended documentation to be included with each premarket submission (see section 524B of the FD&C Act).

2. Changes Unlikely to Impact Cybersecurity

In general, changes unlikely to impact cybersecurity could include material changes, sterilization method changes, or a change to an algorithm without change to architecture/software structure/connectivity.

For these types of changes, FDA recommends that manufacturers of cyber devices provide the following information to meet their premarket submission requirements in section 524B of the FD&C Act:

- 524B(b)(1)
  - If not previously provided, manufacturers must provide a plan as described in section 524B(b)(1) of the FD&C Act; we recommend that it contain the information as described in Section II.C.1., above.
  - If a plan described in Section II.C.1., above, was previously provided, the manufacturer should provide a reference to the prior submission, a summary of any changes to the plan, and summaries of any updates/patches made to address vulnerabilities or exploits.
- 524B(b)(2)
  - Instead of the full documentation described as required or recommended in Section II.C.2., above, manufacturers may provide summary information to provide that there is a reasonable assurance that the device and related systems are cybersecure and no uncontrolled vulnerabilities, as described in Sections III.J. and VII.B. of the FDA guidance "Postmarket Management of Cybersecurity in Medical Devices,"[17] are present. FDA recommends that this information include a summary assessment documenting the statements made in the summary

[16] For more information on FDA's least burdensome provisions, see FDA's guidance The Least Burdensome Provisions: Concept and Principles

[17] Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

assessment, including a summary assessment of any cybersecurity impact from changes made since the last authorization (i.e., Letter to File, Annually Reportable) and a summary assessment of any vulnerabilities identified since the last authorization.

- If there are any limitations to updating the cybersecurity of the cyber device and related systems, the manufacturer should provide a description of the limitations of the system which prevent further cybersecurity controls, an assessment of the residual cybersecurity risk, and an assessment of the benefits and risks of the system.

- 524B(b)(3)
  - Section 524B(b)(3) of the FD&C Act requires manufacturers of cyber devices to provide an SBOM, including commercial, open-source, and off-the-shelf software components. To assist with complying with this requirement, we recommend that a cyber device provide SBOMs that contain the information recommended in Section V.A.4(b) of the Premarket Cybersecurity Guidance.

In general, in its cybersecurity review, FDA intends to focus substantive review on modifications to cybersecurity controls or modifications that are likely to affect cybersecurity. However, regardless of the type of change being proposed to the device in the premarket submission, FDA intends to take into account known cybersecurity concerns that are applicable to such device when conducting its premarket reviews and in determining whether the device has a reasonable assurance of cybersecurity.

E. Reasonable Assurance of Cybersecurity of Cyber Devices

Section 3305(c) of FDORA provides that nothing in section 524B of the FD&C Act "shall be construed to affect the Secretary's authority related to ensuring that there is a reasonable assurance of the safety and effectiveness of devices, which may include ensuring that there is a reasonable assurance of the cybersecurity of certain cyber devices . . ." FDA interprets this provision to mean that a "reasonable assurance of cybersecurity" can be part of FDA's determination of a device's safety and effectiveness. Moreover, a determination that there is a reasonable assurance of cybersecurity is relevant to the various premarket pathways and authorization under them, specifically, FDA's review of a PMA, PDP, De Novo, HDE, and 510(k). With the exponential growth of interconnected devices on the market over the past few years (see Section I. of the Premarket Cybersecurity Guidance), ensuring cybersecurity has become essential to FDA's ability to protect the public health and provide reasonable assurance of safety and effectiveness of devices.

When evaluating a 510(k) submission, FDA considers changes to the environment of use (e.g., changes in technology the subject device will interact with or operate within, and any new risks or vulnerabilities the device will be exposed to), new risks or vulnerabilities in the technological characteristics compared to the predicate device submission (e.g., changes to level of support for component software, vulnerabilities in communication protocols or technology used by the subject device), and how the subject device design and/or performance testing address these new

risks or vulnerabilities.[18] For example, if in reviewing the 510(k) for an alarm for a central nursing station software, FDA identifies that the device has increased risks compared to its predicate because it does not have the necessary encryption to protect against a recently identified cyber threat, FDA may ask for additional performance data. If the data provided is inadequate, FDA would likely make a determination that the new device is not substantially equivalent (NSE) to the predicate device because this threat, if exploited, could negatively impact the safety and effectiveness of the device because alarm accuracy is essential for health care providers to effectively monitor the health of patients in a hospital.

[18] For more information about current review practices for 510(k) submission, see FDA's guidance The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)]