Welcome To Today’s Webinar

Thanks for joining us!
We’ll get started in a few minutes

Today’s Topic:
Draft Guidance - Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act

April 30, 2024

Draft Guidance - Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act

Matthew Hazelett

Senior Cybersecurity Policy Analyst

OPEQ Digital Health Staff

Office of Product Evaluation and Quality

Center for Devices and Radiological Health

U.S. Food and Drug Administration

Draft Guidance - Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act

Matthew Hazelett
Senior Cybersecurity Policy Analyst
OPEQ Digital Health Staff
Office of Product Evaluation and Quality

Center for Devices and Radiological Health
U.S. Food and Drug Administration

Draft Guidance

- **Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act**
  - www.fda.gov/regulatory-information/search-fda-guidance-documents/select-updates-premarket-cybersecurity-guidance-section-524b-fdc-act

Learning Objectives

- Describe proposed interpretations of key terms from Section 524B of the Food, Drug & Cosmetic (FD&C) Act
- Describe proposed recommendations of what to provide in premarket submissions for each 524B requirement
- Describe proposed recommendations of what to provide in premarket submissions for modifications to existing devices
- Describe FDA's proposed thoughts on how 524B fits into existing regulatory submission pathways

Background

Background

- Provides interpretation of elements from Section 524B of the FD&C Act that couldn’t be included in the final guidance, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (September 2023)
- When finalized, content from Section II of this Select Update will be added as Section VII to the Premarket Cybersecurity Guidance

Proposed Interpretations of Key Terms

Cyber Device

- FDA considers:
  - A “cyber device” to include devices that are or contain software, including software that is firmware or programmable logic.
  - 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 of the device and the environment of use).

Cyber Device (cont)

- 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.
- FDA considers devices that include 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 (for example, USB, ethernet, serial port).

Related System

- 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,
  – Software/firmware update servers, and
  – Connections to health care facility networks.

Coordinated Vulnerability Disclosure and Related Procedures

- 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.

Proposed Premarket Submission Documentation Recommendations for 524B Requirements

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

- Information recommended for the Cybersecurity Management Plan described in Section VI.B. of the Premarket Cybersecurity Guidance
- Details on CVD and Related Procedures
- Describe the timeline with associated justifications to develop and release required updates and patches
- Plan for maintaining documentation as new information becomes available
- Documentation should account for any differences in the risk management for fielded devices (such as differences between marketed devices and devices no longer marketed but still in use)

Reasonable Assurance of Cybersecurity (524B(b)(2))

- The documentation recommendations identified in the Premarket Cybersecurity Guidance and summarized in Appendix 4 of the Premarket Cybersecurity Guidance should be considered and used to demonstrate reasonable assurance that the device and related systems are cybersecure

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

- Recommend to provide SBOMs that contain the information recommended in Section V.A.4(b) of the Premarket Cybersecurity Guidance

Proposed Premarket Submission Documentation Recommendations for Modifications

Proposed Types of Changes

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.

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.

Changes that May Impact Cybersecurity

- For these types of changes, see Section II.C. of the Select Update (all documentation identified in prior slides for new submissions) for required and recommended documentation to be included with each premarket submission.

Changes Unlikely to Impact Cybersecurity

- For these types of changes, FDA has proposed recommended documentation for each of the 524B requirements:
  - 524B(b)(1)
    - If a plan was 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. of the Select Update Guidance
    - If a plan 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.

Changes Unlikely to Impact Cybersecurity (cont)

- 524B(b)(2)
  - Instead of the full documentation described previously, 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 identified in the Postmarket Cybersecurity Guidance
    - FDA recommends that this information include a summary assessment, including a summary assessment of any cybersecurity impact from changes made since the last authorization (such as Letter to File or Annually Reportable) and a summary assessment of any vulnerabilities identified since the last authorization.

Changes Unlikely to Impact Cybersecurity (cont)

- 524B(b)(2)
  - 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.

Changes Unlikely to Impact Cybersecurity (cont)

- 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.

Proposed Thinking on 524B and the Regulatory Submission Pathways

Reasonable Assurance of Cybersecurity

- Section 3305(c) of the Food and Drug Omnibus Reform Act (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.

Reasonable Assurance of Cybersecurity (cont)

- 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 Premarket Approval (PMA) Application, Product Development Protocol (PDP), De Novo, Humanitarian Device Exemption (HDE), and Premarket Notification (510(k)).

Cybersecurity in 510(k) Submissions

- When evaluating a 510(k) submission, FDA considers:
  - Changes to the environment of use (such as 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 (such as 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.

510(k) Example

- 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.

Resources

Slide Number	Cited Resource	URL
7, 14, 15, 16, 23	Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
11	Multiple Function Device Products: Policy and Considerations	www.fda.gov/regulatory-information/search-fda-guidance-documents/multiple-function-device-products-policy-and-considerations
21	Postmarket Management of Cybersecurity in Medical Devices	www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

A Note about Draft Guidances

- You may comment on any guidance at any time
  - see 21 CFR 10.115(g)(5)
- Please submit comments on draft guidance before closure date
  - to ensures that FDA considers your comment on a draft guidance before we work on final guidance

Summary

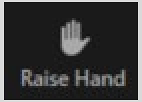
- Guidance includes proposed interpretations of key terms used in Section 524B of the FD&C Act
- Each 524B requirement has required and/or recommended documentation
- Submission documentation for modifications to existing devices will generally differ based on the type of change
- Providing a reasonable assurance that device and related systems are cybersecure will be assessed as part of FDA's existing regulatory submission evaluation process

U.S. FOOD & DRUG ADMINISTRATION

Additional Panelist

Jessica Wilkerson
Senior Cyber Policy Advisor and Medical Device Cybersecurity Team Lead
Division of Medical Device Cybersecurity
Office of Readiness and Response
Office of Strategic Partnerships and Technology Innovation

Let's Take Your Questions

- **To Ask a Question:**
  1. Raise your hand in Zoom 

  2. Moderator will announce your name and invite you to ask your question
  3. Unmute yourself when prompted in Zoom to ask your question

- **When Asking a Question:**
  - Ask one question only
  - Keep question short
  - No questions about specific submissions

- **After Question is Answered:**
  - Mute yourself and lower your hand
  - If you have more questions - raise your hand again

Thanks for Joining Today!

- **Presentation and Transcript will be available at CDRH Learn**
  - www.fda.gov/Training/CDRHLearn
- **Additional questions about today's webinar**
  - Email: DICE@fda.hhs.gov
- **Upcoming Webinars**
  - www.fda.gov/CDRHevents

Start Here/The Basics! (Updated Module 10/16/2023)
MDUFA Small Business Program, Registration and Listing

How to Study and Market Your Device - *(Updated 11/20/23)*
510k, De Novo, IDE, PMA, HUD/HDE, Q-Submissions, Standards, Classification

Postmarket Activities
Quality System, Exporting, Device Recalls, MDR, Inspection - Global Harmonization

In Vitro Diagnostics - *(Updated 12/19/23)*
IVD Development, CLIA, and Virtual Town Hall Series

Unique Device Identification (UDI) System

Specialty Technical Topics - *(Updated 4/1/24)*

Radiation-Emitting Products

510(k) Third Party Review Program (for Third Party Review Organizations)

Industry Basics Workshop Series

FDA

U.S. FOOD & DRUG

ADMINISTRATION