Justin Post

AMDM's 2023 IVD Hybrid Focus Meeting

October 20th, 2023

FDA PREMARKET CYBERSECURITY – SECTION 524B AND FINAL GUIDANCE

Why is Cybersecurity Important?

Cybersecurity is a part of Safety and Effectiveness

FDA has found 510(k) submissions to be “not substantially equivalent” (NSE) and Premarket Approval (PMA) devices to be “not approvable” based on cybersecurity concerns alone.

Section 524B of FD&C Act

- The Consolidated Appropriations Act for 2023 was signed into law December 29, 2022 and includes the Food and Drug Omnibus Reform Act (FDORA)
- Section 3305 of Omnibus – Ensuring Cybersecurity of Medical Devices
- Adds New Section 524B of the FD&C Act – Ensuring Cybersecurity of Devices
- Applies to prospective submissions for ‘cyber devices’ under the 510(k), de Novo, HDE, PDP, and PMA pathways
- Effective 90 days after signing (March 29, 2023)

524B(c) - Cyber Device

Section 524B(c) defines a Cyber Device as a device that:

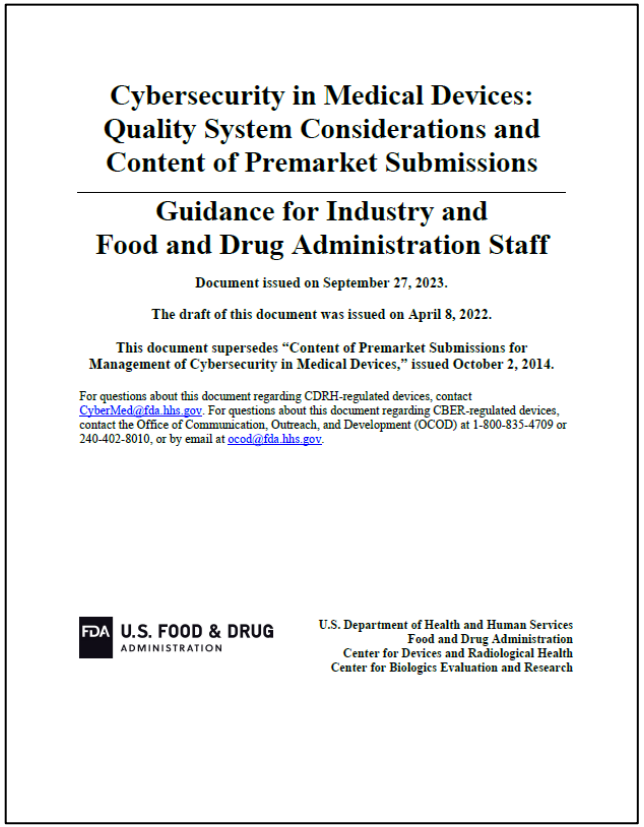
1. Includes software validated, installed, or authorized by the sponsor as a device or in a device;
2. Has the ability to connect to the internet; and
3. Contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats

524B Requirements

- Section 524B(a) requires that a sponsor of an application (of the aforementioned submission types) provide the documentation required described in subsection (b)
- Section 524B(b) requires manufacturers of cyber devices to:
  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

FDA Final Premarket Guidance

- Published on September 26, 2023
- Recommendations are intended to help manufacturers comply with requirements under Section 524B of the FD&C Act
- Addresses how cybersecurity fits into the Quality System Requirements (21 CFR Part 820) and premarket submission documentation requirements
- Public Webinar on November 2, 2023
- A detailed walkthrough of the guidance and 524B content is forthcoming in eSTAR



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

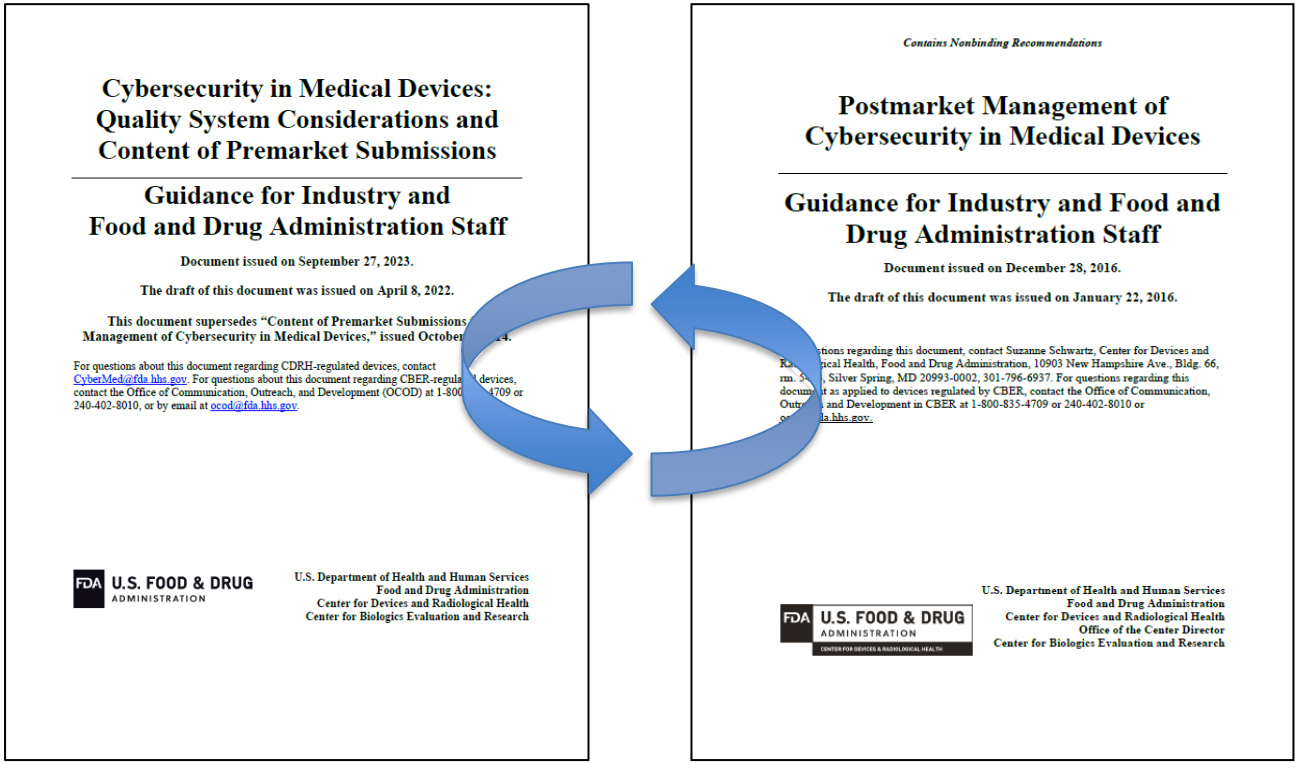
This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

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.

FDA 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

FDA Final Cybersecurity Guidance



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions/ Management of Cybersecurity in Medical Devices," issued October

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

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

Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

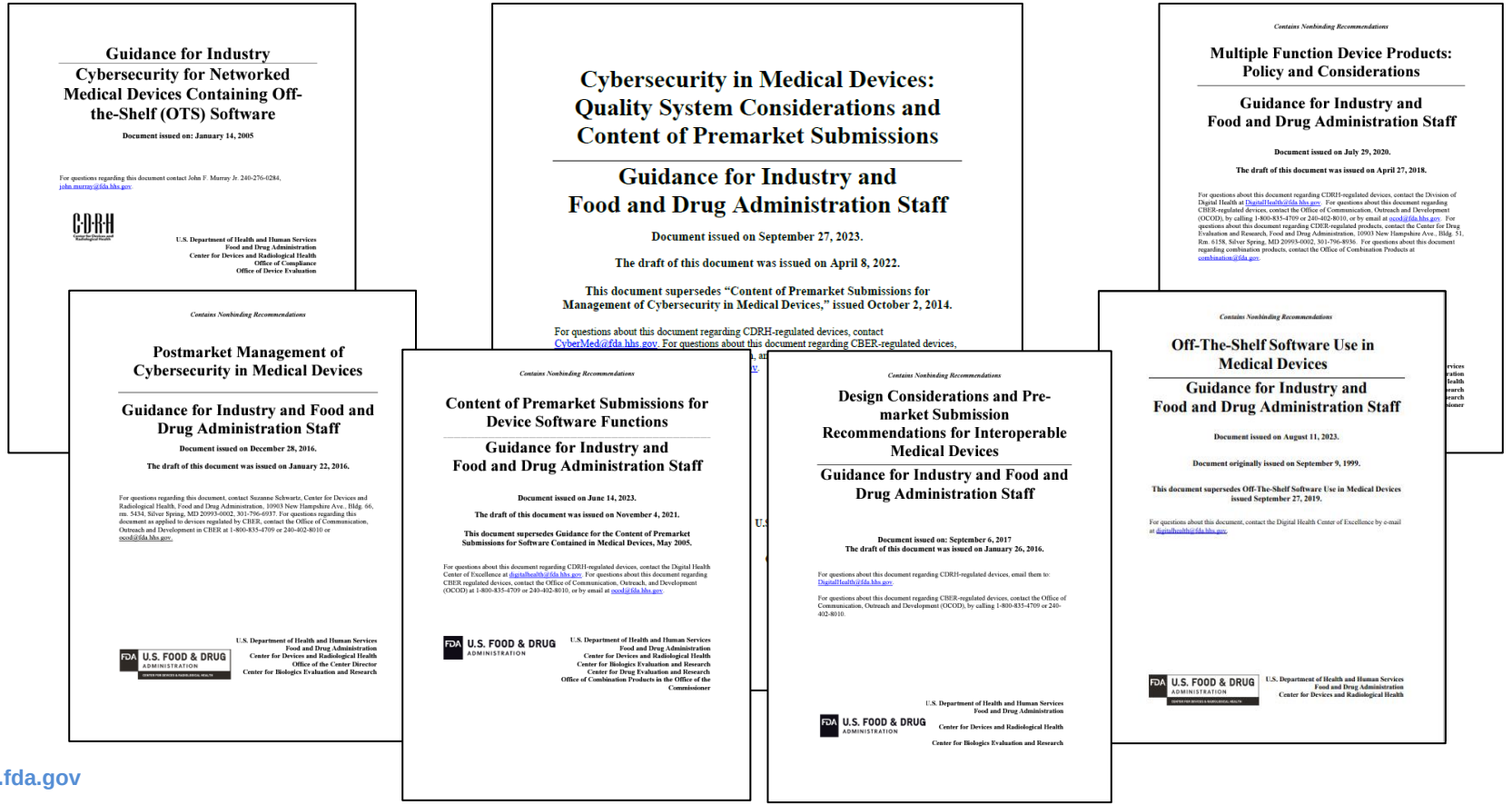
The draft of this document was issued on January 22, 2016.

tions regarding this document, contact Suzanne Schwartz, Center for Devices and R rical Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5 , Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this docum t as applied to devices regulated by CBER, contact the Office of Communication, Outr and Development in CBER at 1-800-835-4709 or 240-402-8010 or o da.hhs.gov.

U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

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

Premarket Reviews Today



Does Cybersecurity Apply?

- Cybersecurity applies if the device is or contains software
- Cybersecurity documentation is required if the device meets the definition of a Cyber Device
- Cybersecurity considerations apply regardless of whether the software or software component was designed by the medical device manufacturer or a third-party
- Risks **increase** if device contains one or more of these example interfaces:
  - Wired: USB, ethernet, SD, CD, RGA, etc. or
  - Wireless: Wi-Fi, Bluetooth, RF, inductive, Cloud, etc.
- Cybersecurity considerations apply for entire system, not just end device. Examples include:
  - Software update infrastructure
  - Cloud applications
  - Commercial devices (phones, tablets, computers, etc.)

Guidance Documentation for Reviews

- Security Risk Management
- Security Architecture
- Cybersecurity Testing
- Labeling
- Cybersecurity Management Plan

Guidance Documentation for Reviews

Security Risk Management

- Security risk management applies to the context of the larger system in which the device operates and should be integrated across the TPLC
  - This is an end-to-end assessment of cybersecurity risks and controls
- Parallel but interfacing process with ISO 14971 Safety Risk Management
- Manufactures should provide their Security Risk Management Report in Premarket Submissions
  - See AAMI TIR57:2016 for more details

Security Risk Management

- Threat Modeling
- Cybersecurity Risk Assessment
- Interoperability
- Third-Party Software Components (SBOM)
- Unresolved Anomalies
- TPLC Security Risk Management (Metrics)

Security Risk Management

Third-Party Software Components (SBOM)

- Recommendations align with October 2021 National Telecommunications and Information Administration (NTIA) Multistakeholder Process on Software Component Transparency document "Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)"
  - Recommend a machine-readable version be provided
- Additional supporting documentation can be provided in the submission separate from the SBOM
  - Component Support Information
  - Vulnerability Assessment

Guidance Documentation for Reviews

Security Architecture

- Implementation of Security Controls
  - Security needs to be designed in
  - 8 Control Categories
  - Appendix 1 contains recommendations for each category
- Architecture Views
  - 4 Types of Views
    - Global System View
    - Multi-Patient Harm View
    - Updateability/Patchability View
    - Security Use Case View(s)
  - Appendix 2 contains recommendations for the level of detail for the views

Guidance Documentation for Reviews

Cybersecurity Testing

- Recommendations on Types of Testing:
  - Security Requirement Testing
  - Threat Mitigation
  - Vulnerability Testing
  - Penetration Testing
- Section also makes recommendations on:
  - Independence and technical expertise of testers
  - Scope of testing (i.e., system-level)
  - Third-Party Testing recommendations
  - Submission documentation

Guidance Documentation for Reviews

Labeling

- Can be provided in different locations depending on appropriate users for the information (manual vs. security implementation guide)
- 14 recommended elements
- Labeling mitigations and risk transfer items may need to be included as part of Human Factors Testing tasks
- Focus on ensuring users have sufficient information on device to integrate it and have sufficient information to manage security risks and updates

Guidance Documentation for Reviews

Cybersecurity Management Plan

- Includes managing cybersecurity throughout lifecycle inclusive of vulnerabilities and incidents
- Plans should include Coordinated Vulnerability Disclosure process as described in the 2016 Postmarket Guidance
- Also includes items like:
  - Periodic security testing to test identified vulnerability impact
  - Timeline to develop and release patches as outlined in 524B(b)(2)(A-B) for cyber devices
  - Patching capability (i.e., rate at which updates can be delivered to devices)

Questions?