U.S. FOOD & DRUG ADMINISTRATION

Welcome To Today's Webinar

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

Today's Topic:

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

November 2, 2023

U.S. FOOD & DRUG ADMINISTRATION

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

Matthew Hazelett
Cybersecurity Policy Analyst

Clinical and Scientific Policy Staff
Office of Product Evaluation and Quality

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

Final Guidance

- **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

Learning Objectives

- Describe scope of the guidance
- Describe general principles in the guidance
- Describe design and documentation recommendations
- Describe transparency recommendations
- Describe changes and updates from the 2022 draft guidance

Scope

- **This guidance document is applicable to devices that contain software (including firmware) or programmable logic, as well as devices that have a device software function.**
  - Devices within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) whether or not they require a premarket submission
  - Guidance is not limited to devices that are network-enabled or contain other connected capabilities.

Scope (cont.)

- **Applicable Submission Types to CDRH and CBER:**
  - Premarket Notification (510(k)) submissions
  - De Novo Classification Requests
  - Premarket Approval Applications (PMAs) and PMA supplements
  - Product Development Protocols (PDPs)
  - Investigational Device Exemption (IDE) submissions
  - Humanitarian Device Exemption (HDE) submissions
  - Biologics License Application (BLA) submissions – **New**
  - Investigational New Drug (IND) submissions – **New**

CBER – Center for Biologics Evaluation and Research

Section 524B of the Federal Food, Drug, and Cosmetic (FD&C) Act

Section 524B of the FD&C Act

- Consolidated Appropriations Act for 2023 was signed into law December 29, 2022; includes Food and Drug Omnibus Reform Act (FDORA) which adds Section 524B to the FD&C Act
- Went into effect on March 29, 2023
- Applies to prospective submissions for ‘cyber devices’ under the 510(k), De Novo, HDE, PDP, and PMA pathways
- Guidance documentation recommendations intended to help manufacturers comply with requirements under Section 524B

Section 524B – Cyber Device

- 524B(c) defines a Cyber Device as a device that:
  - Includes software that a sponsor has validated, installed, or authorized as a device or in a device;
  - Has ability to connect to the internet; and
  - Contains any such technological characteristics a sponsor has validated, installed, or authorized that could be vulnerable to cybersecurity threats

Section 524B – Requirements

- Section 524B(b) requires sponsors of a cyber device application to provide documentation for the following:
  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

Section 524B – Requirements (cont.)

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

General Principles

General Principles

A. Cybersecurity is Part of Device Safety and the Quality System (QS) Regulation

- Cybersecurity is a part of safety and effectiveness
- Cybersecurity aligns with the QS Regulation
- A Secure Product Development Framework (SPDF) can be used to fulfill aspects of QS Regulation

B. Designing for Security

- “Design in” rather than “bolt on” cybersecurity controls
- Outlines key security objectives medical devices should achieve

General Principles

C. Transparency

- Importance of end user having cybersecurity information to ensure continued safe use of the device

D. Submission Documentation

- Recommendations complement and are in addition to the software premarket guidance
- Documentation expected to scale with cybersecurity risk of device

Design and Documentation Recommendations

Design Recommendations

- **Security Objectives for Design:**
  - Authenticity, which includes integrity
  - Authorization
  - Availability
  - Confidentiality
  - Secure and timely updateability and patchability

Design Recommendations

- 8 Security Control Categories to help in meeting the Security Objectives
- Appendix 1 provides specific control recommendations and implementation guidance for consideration to avoid common pitfalls
- Appendices are part of the document recommendations

Documentation Recommendations

- **Section V. Using an SPDF to Manage Cybersecurity Risks**
  - A. Security Risk Management
  - B. Security Architecture
  - C. Cybersecurity Testing
- **Section VI. Cybersecurity Transparency**
  - A. Labeling Recommendations
  - B. Cybersecurity Management Plans

Security Risk Management

- System-level assessment
- Security risk management distinct from safety risk management but the two processes should feed into and out of one another
- Known vulnerabilities should be assessed as reasonably foreseeable
- Risk transfer should only occur if all relevant information is known, assessed, and communicated to users
- Provide a Security Risk Management Report in premarket submissions
  - Described in the Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR57) with additional details in guidance

Security Risk Management (cont.)

1. **Threat Modeling**
   - Includes full system and lifecycle of the device
   - May include Architecture Views
2. **Cybersecurity Risk Assessment - New**
   - Use of exploitability instead of probability
3. **Interoperability Considerations - New**
   - Cybersecurity controls should not be intended to prohibit users from accessing device data
4. **Third Party Software Components**
   - Software bill of materials (SBOM) and vulnerability assessment
5. **Security Assessment of Unresolved Anomalies**
   - Anomalies can present a different vector to safety risks through cybersecurity
6. **Total Product Lifecycle (TPLC) Security Risk Management**
   - Maintain resources and documentation
   - Track and monitor cybersecurity measures and metrics

Software Bill of Materials (SBOM)

- Required for cyber device submissions [See 524B(b)(3)]
- Manufacturers should provide:
  - Machine-readable SBOMs
  - Consistent with minimum elements (also referred to as “baseline attributes”) identified in 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).
- SBOMs provided to users in labeling can conform with industry-accepted formats

SBOM (cont.)

- Manufacturers should also provide:
  - Software level of support provided through monitoring and maintenance from the software component manufacturer
  - Software component's end-of-support date
  - A safety and security risk assessment of each known vulnerability (including device and system impacts)
  - Details of applicable safety and security risk controls to address the vulnerability
  - Note: this additional information *does not* have to be included in the SBOM, but can be provided separately, to support tool ingestion and machine readability

SBOM (cont.)

- Sources of vulnerability information includes:
  - Software component suppliers
  - Vulnerability databases (Example: National Institute of Standards and Technology's (NIST) National Vulnerability Database)
  - Cybersecurity & Infrastructure Security Agency's (CISA) Known Exploited Vulnerability (KEV) Catalog

Architecture Views

- Can be part of Threat Modeling Documentation
- 4 View Categories
    a) Global System View
    b) Multi-Patient Harm View
    c) Updateability/Patchability View
    d) Security Use Case View(s)
        – Operational states and different clinical use cases

Architecture Views

- These security architecture views should:
  - Identify security-relevant system elements and their interfaces;
  - Define security context, domains, boundaries, and external interfaces of system;
  - Align architecture with (a) system security objectives and requirements, (b) security design characteristics; and
  - Establish traceability of architecture elements to user and system security requirements.

- Level of recommended detail for the architecture views captured in Appendix 2 including:
  - Diagrams
  - Information Details for an Architecture View

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 (that is, system-level)
  - Third-Party Testing recommendations
  - Submission documentation

Transparency: Labeling and Cybersecurity Management Recommendations

Labeling Recommendations

- Largely similar to recommendations proposed in 2022 Draft Guidance with some changes and reordering
- Can be provided in different locations depending on appropriate users for the information (manual versus security implementation guide)
- 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

Cybersecurity Management Plans

- Required for cyber device submissions [See 524B(b)(1)]
- 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
  - Patching capability (that is, rate at which updates can be delivered to devices)

Key Changes From 2022 Draft Guidance

Key Changes

- **Expanded scope**
  - Included CBER submission types
  - Included considerations for combination products
  - Added elements associated with the requirements under Section 524B of the FD&C Act
- **Structure Changes**
  - Added new subsections in Security Risk Management section to clarify premarket submission documentation deliverables including Cybersecurity Risk Assessment and Interoperability
  - Added Appendix 4 to further clarify premarket submission documentation recommendations
- **Software Bill of Materials (SBOM)**
  - Alignment with 2021 NTIA SBOM Framing Document
  - Supporting materials can be separate from the SBOM

Future Guidance

Future Guidance

- **Draft Select Update**
  - Will provide details on 524B interpretation
  - On CDRH's A-List for FY2024 priorities

Resources

Slide Number	Cited Resource	URL
14	Premarket Software Guidance: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices	www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-content-premarket-submissions-software-contained-medical-devices
21	NTIA's Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)	www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf
29	2016 Postmarket Guidance: Postmarket Management of Cybersecurity in Medical Devices	www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

Summary

- General principles in Section IV outline core concepts in guidance
- Design recommendations focus on security objectives and that documentation will scale with cybersecurity risk
- Transparency of device cybersecurity recommendations include proactive labeling and plans to respond to emerging issues throughout the total product lifecycle
- This final guidance reflects updates made due to comments provided on the 2022 Draft and new requirements under Section 524B of the FD&C Act


FDA
U.S. FOOD & DRUG
ADMINISTRATION

Additional Panelists

Aftin Ross
Acting Deputy Division Director

Division of All Hazards Response, Science and Strategic Partnerships
Office of Strategic Partnerships and Technology Innovation

Jessica Wilkerson, J.D.
Senior Cyber Policy Advisor and Medical Device Cybersecurity Team Lead

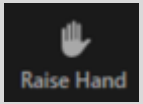
All Hazards Readiness Response & Cybersecurity Team
Division of All Hazards Response, Science and Strategic Partnerships
Office of Strategic Partnerships and Technology Innovation

Erin Quencer
Regulatory Policy Analyst

Office of Policy

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

Let's Take Your Questions

- **To Ask a Question:**
  1. Please "Raise Your Hand" 

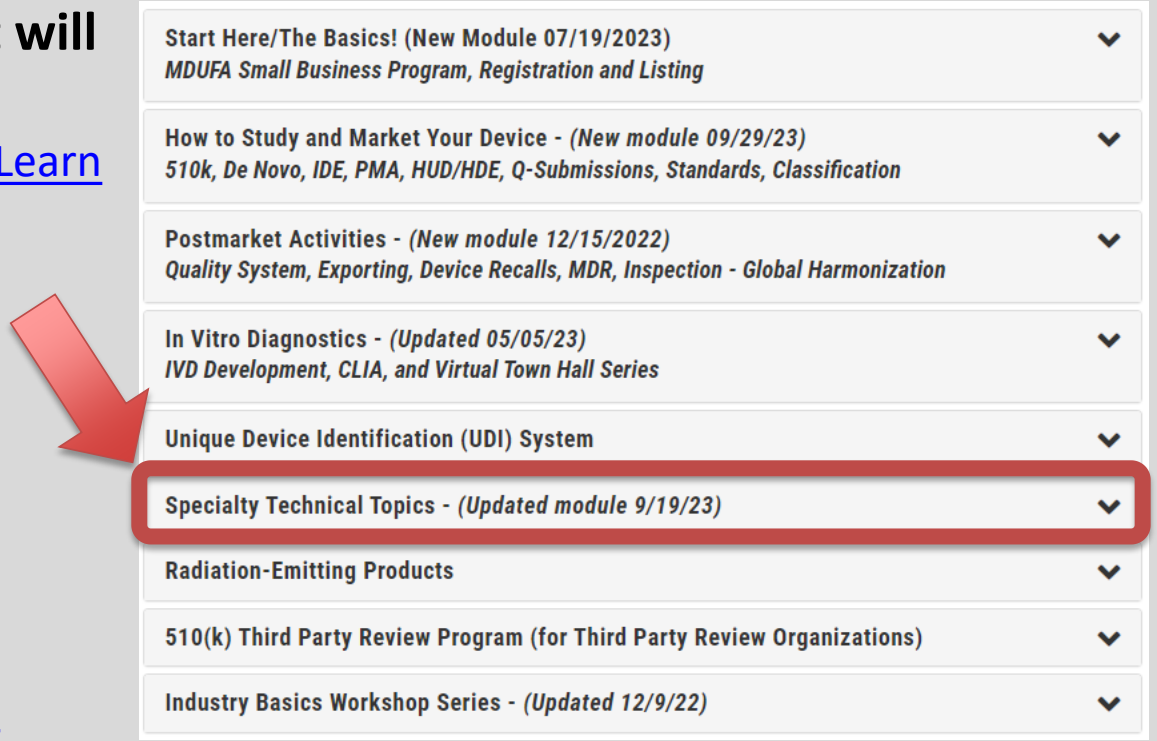
  2. Moderator will Announce Your Name to Invite You to Ask Your Question
  3. Unmute yourself when called

- **When Asking a Question:**
  - Ask 1 question only
  - Keep question short
  - No questions about individual submissions

- **After Question is Answered:**
  - Please mute yourself again
  - 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 presentation**
  - Email: DICE@fda.hhs.gov
- **Upcoming Webinars**
  - www.fda.gov/CDRHWebinar




FDA
U.S. FOOD & DRUG
ADMINISTRATION