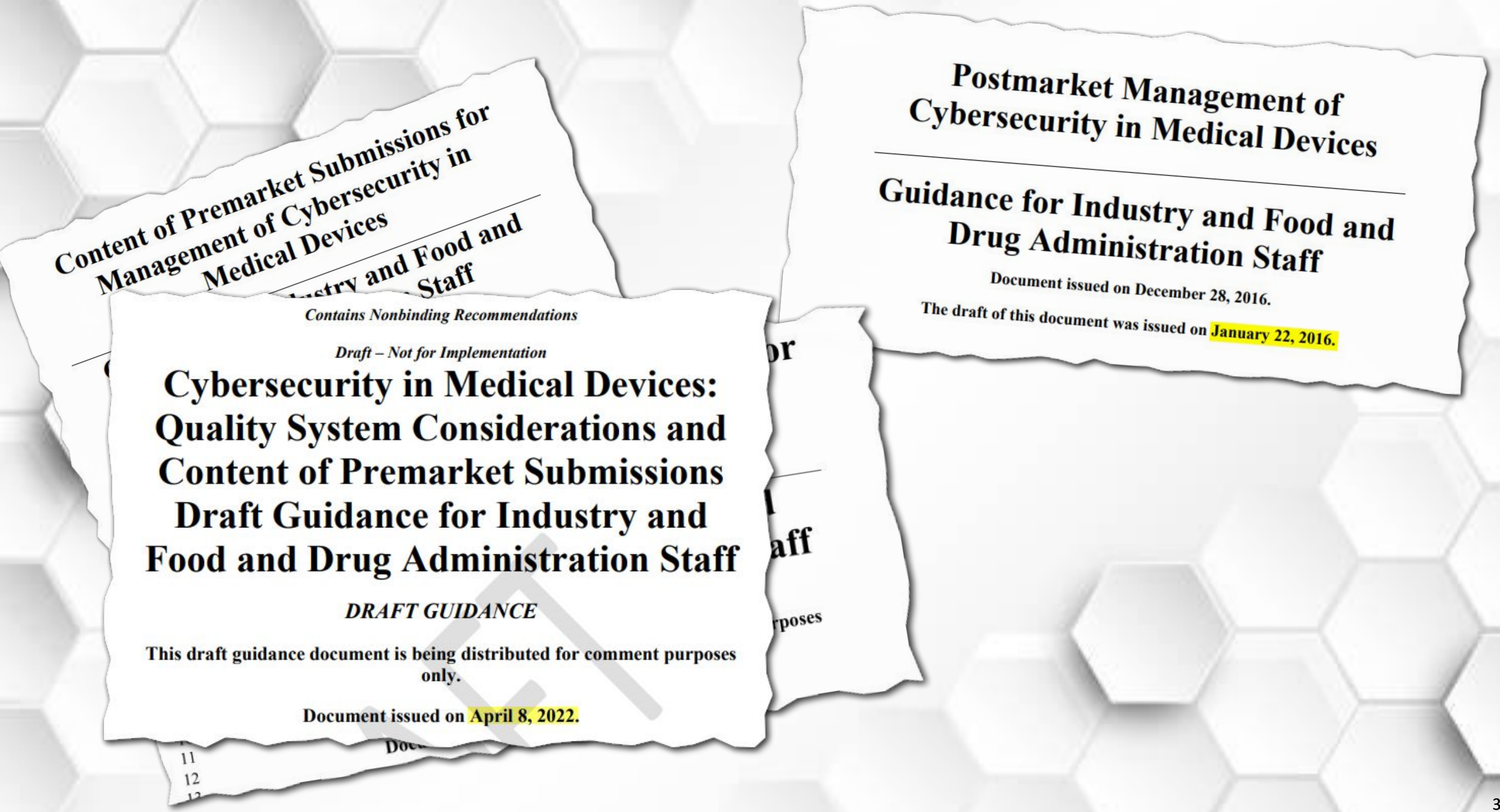
Cybersecurity Regulation in 2023 and Beyond

What Every Manufacturer Needs to Know

Chris Reed
Vice President of Product Security
Medtronic
Chair of HSCC's JSP v2

Christopher Gates
Director of Product Security
Velentium
Too many working groups to list

Ken Hoyme
CEO Dark Star Consulting
Failed at retirement from Boston Scientific
MedCrypt Board of Advisors
UMN Instructor
Too many working groups to list


Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
Guidance for Industry and Food and Drug Administration Staff
Contains Nonbinding Recommendations
Draft – Not for Implementation
Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff
DRAFT GUIDANCE
This draft guidance document is being distributed for comment purposes only.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 April 8, 2022.
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.

Contains Nonbinding Recommendations

Draft – Not for Implementation

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

The $1.7 trillion Omnibus Appropriations Bill

- Signed into **law** December 29th, 2022
- Amends the Food, Drug, and Cosmetic Act to include medical device cybersecurity
- Applies to new and **modified existing**, but **not** to fielded devices.
- The FDA to finalize Premarket Guidance by the end of 2023
- The FDA and CISA to update the guidance annually

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*

- Manufacturers must submit plans to the FDA to:
  - Monitor, Identify, and address post-market cybersecurity vulnerabilities
  - Coordinated vulnerability disclosure (inc. procedures)
  - Ensure devices are secure
  - Release post-market software/firmware updates and patches
  - Provide SBOMs to the FDA

CYBERSECURITY REQUIREMENTS.—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, post-market 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 post-market 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*

RULE OF CONSTRUCTION.—Nothing in this section, including the amendments made by this section, 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, including for devices approved or cleared prior to the date of enactment of this Act.

- This gives the FDA complete authority to define any aspect of medical device cybersecurity including overriding what is said in the omnibus act itself.
- The FDA still retains the ability to enforce Safety and Effectiveness in fielded devices

- FDA mandate for medical device cybersecurity took effect March 29th 2023
  - From March 29th until October 1st 2023 (The “friendly” period)
    - The premarket reviewer will ask review questions and cite deficiencies resulting from the premarket application review process.
    - This enables manufacturers to correct areas they may have missed and should result in delays rather than rejections “if” manufacturers can demonstrate compliance with the new cybersecurity requirements within the 180 calendar day period.
  - From October 1st 2023 onward
    - The Refuse To Accept (RTA) checklist will be used by receiving clerks (within 15 calendar days) who will reject submissions that do not contain all of the cybersecurity artifacts

eSTAR

Starting October 1, 2023, all 510(k) submissions unless exempted* must be submitted as electronic submissions using eSTAR.

*As noted in the final guidance, Electronic Submission Template for Medical Device 510(k) Submissions, all 510(k) submissions including original submissions for Traditional, Special, and Abbreviated 510(k)s, and subsequent Supplements and Amendments and any other subsequent submissions to an original submission, unless exempted in *Section VI.A Waivers and Exemptions From Electronic Submission Requirements* of the guidance, are required to be submitted as electronic submissions. The electronic submission template, eSTAR, is the only currently available electronic submission template to facilitate the preparation of 510(k) electronic submissions.

https://www.fda.gov/medical-devices/how-study-and-market-your-device/voluntary-estar-program

eSTAR Artifacts

JavaScript Window

Manufacturers are required to provide certain information in their premarket submissions per Section 524B of the FD&C Act. The 2014 Premarket Cybersecurity Guidance discusses the following activities as part of the validation and risk analysis for cybersecurity (Section 4), which may be helpful in providing the required information:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

Risk management for cybersecurity includes an assessment of the system to understand the parts of the device that are vulnerable to a cybersecurity attack (often referred as "the attack surface" in cybersecurity literature) along with the assessment of the assets, vulnerabilities, and risk controls employed. The compilation of the assets, vulnerabilities, and risk controls are collectively called the threat model.

The concepts (Identify, Protect, Detect, Respond, and Recover) in Section 5 of the 2014 Premarket Cybersecurity Guidance should be incorporated into the risk management documentation.

The concepts (Vulnerabilities/Risks, Controls, Traceability Matrix, Malware-Free Shipping) in Section 6 of the Premarket Cybersecurity Guidance should be incorporated into the risk management.

Resources

Threat Modeling | Cybersecurity Risk Assessment | Unresolved Anomalies | Cybersecurity Controls | Traceability Matrix | Cybersecurity Testing | SBOM and Supporting Info

OK

The April 2022 Premarket Guidance

Content For Premarket Submission
2018 Premarket Guidance

Security risk management plan
Threat Modeling: interfaces
Security architecture views: Communications/Networking
Security architecture views: security use case
TPSC any known vulnerabilities & risk assessment
SBOM
Security risk management report
Vulnerability testing

Content For Premarket Submission
eSTAR

Cybersecurity Management Plan
Threat Modeling
Cybersecurity Risk Assessment
Unresolved Anomalies
Cybersecurity Controls
Ensure Trusted Content
Detect, Respond, Recover
Trace cybersecurity controls to vulnerabilities and tests
Development Frameworks and Testing
SBOM and supporting information
Hazard Analysis for Off The Shelf Software
Cybersecurity Labeling

Content For Premarket Submission
2022 Premarket Guidance

Security risk management plan
SPDF selection and justification
Threat Modeling: supply chain
Threat Modeling: manufacturing
Threat Modeling: deployment
Threat Modeling: interfaces
Threat Modeling: maintenance/updates
Threat Modeling: decommissioning activities
Rationale for threat modeling methodologies utilized
Security architecture views: Device hardware
Security architecture views: Configuration and other devices
Security architecture views: HDO environment
Security architecture views: Communications/Networking
Security architecture views: Connected servers
Security architecture views: Global system
Security architecture views: multi-patient harm
Security architecture views: updateability
Security architecture views: security use case
Security architecture views: sequence diagrams

Supply Chain Vendor Assessments
Third Party Software Component (“TPSC”) Management
TPSC level of support by mfg.
TPSC EOS date
TPSC any known vulnerabilities & risk assessment
TPSC Describe method of identifying vulnerabilities
TPSC vulnerability compensating controls
SBOM
MDS2
List of all software anomalies
Risk assessment of all anomalies becoming vulnerabilities
Risk management documentation for multiple in field versions
Metrics: defect density
Metrics: time period from awareness to update
Metrics: time period of update penetration
Tracing from security design inputs to implementation to testing
Testing of effectiveness of security controls
Vulnerability testing
Security risk management report