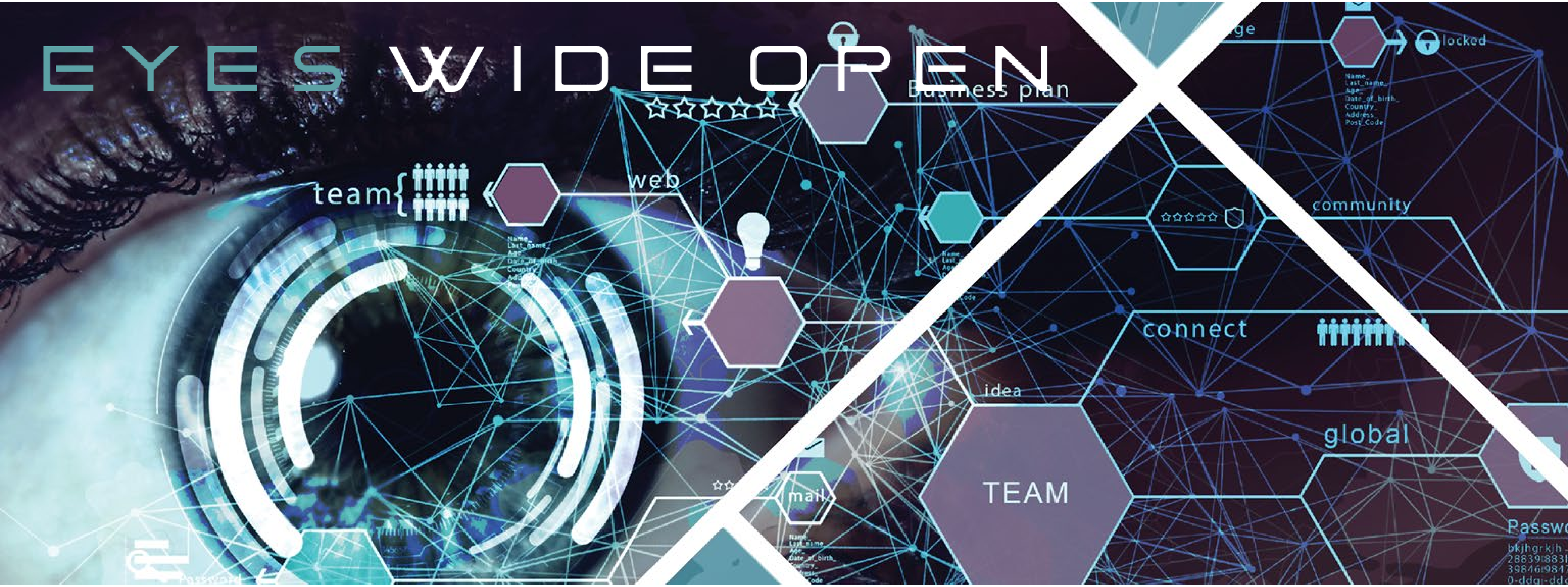
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



12th Annual Cyber Security Summit | October 24-26, 2022

cybersecuritysummit.org

Highlights from the new FDA Premarket Cybersecurity Guidance: Impacts that Medical Device Manufacturers Need to Know

Michelle Jump, CEO, MedSec

Matthew Hazelett, Cybersecurity Policy Analyst, FDA

Speaker Overview

Matthew Hazelett

Cybersecurity Policy Analyst

Clinical and Scientific Policy Staff

Office of Product Evaluation and Quality

FDA

Michelle Jump

CEO

MedSec

MedSec

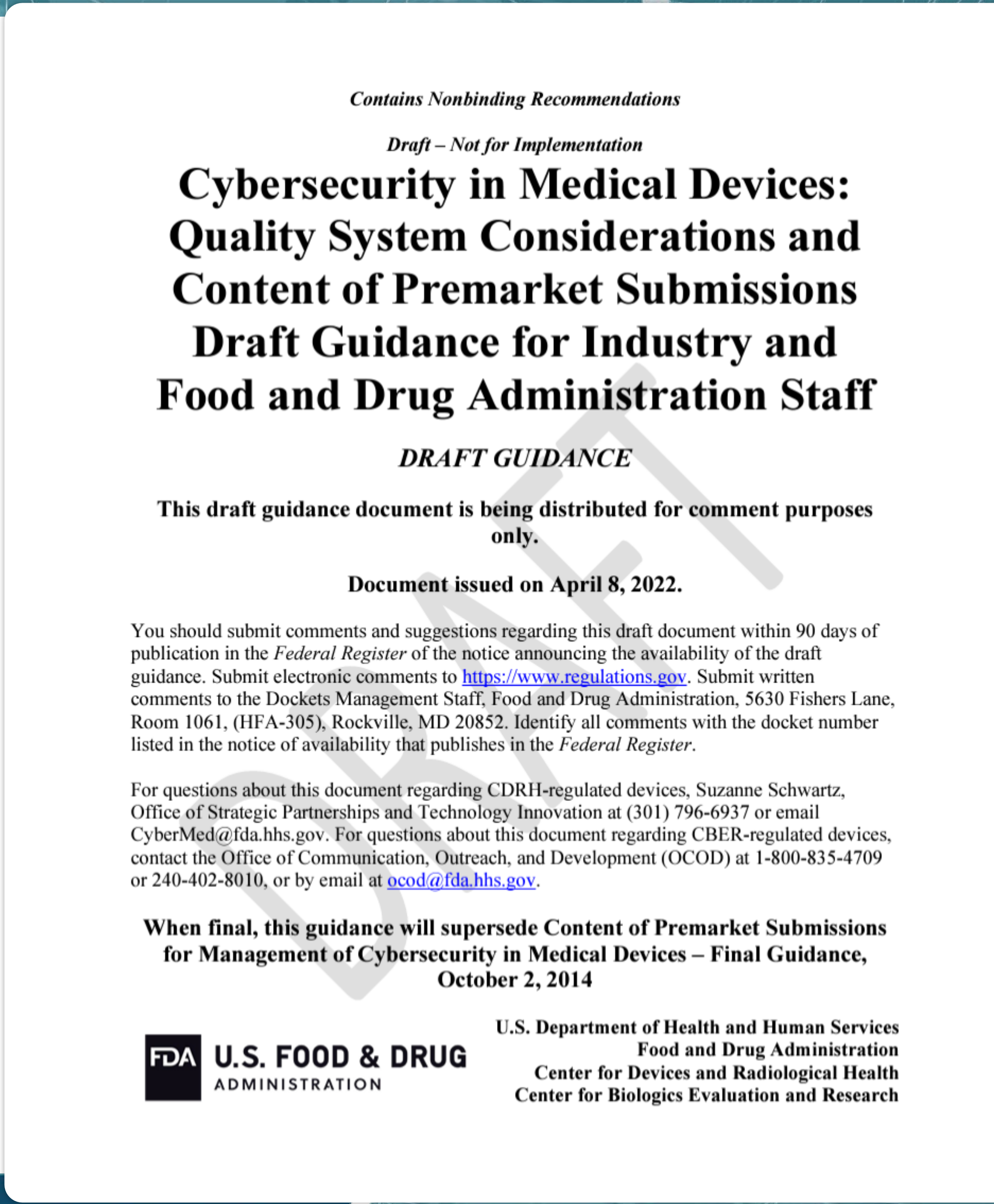
Agenda

The Top Ten Considerations from the New FDA Premarket Guidance

1. Threat modeling
2. SBOM
3. Architectural Views
4. Labeling recommendations
5. SPDF: what is this?
6. Security objectives vs IEC 80001-2-2
7. Security Risk Management
8. No list of documents for submission
9. Why the large number of references to QSR?
10. What is currently expected in submission?

Background

- Current Final FDA Guidance in effect: 2014 Premarket Cyber
- 2018 Draft Guidance released, full update, significantly more detailed
- 2022 FDA Draft Premarket Guidance Released in April 2022 (comments due July 7th)



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Draft – Not for Implementation

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.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

You should submit comments and suggestions regarding this draft document within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance.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. 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, Suzanne Schwartz, Office of Strategic Partnerships and Technology Innovation at (301) 796-6937 or email 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.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

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

A Couple of High-Level Notes

1. Organization

Organization of this guidance is challenging and can be confusing because to the amount of technical content. This 10-step highlight will focus on key areas.

2. Appendices

Are “normative” not “informative: this means that they expect material in Appendices to be met. They were only put in the Appendices for readability due to the high technical nature of the content.

#1: Threat Modeling

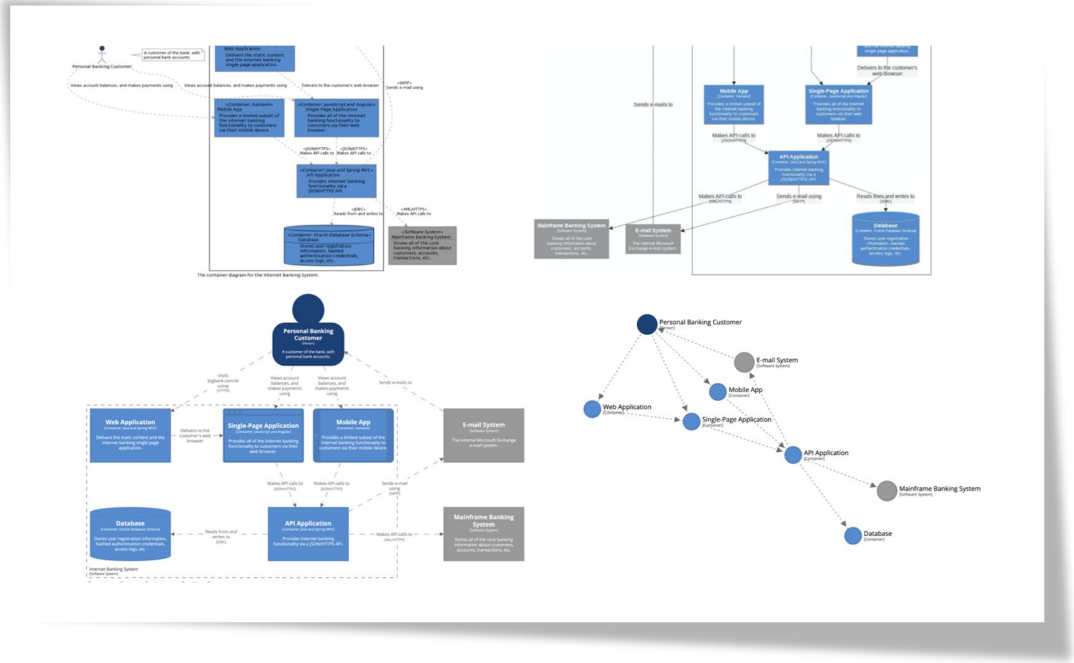
- Design security into product early in the design lifecycle
  - Process helps to ensure completeness
- Essential for security risk management (TIR-57)
- Used to drive abuse cases and ensure coverage in security testing
- FDA expectations
  - Considered required per FDA
  - FDA uses the threat model for more than just threat identification
  - Threat models are beneficial in a regulatory submission to demonstrate how you considered security in designing the product

#2: Software Bill of Materials (SBOM)

- SBOM efforts have been underway since 2018 through NTIA and now CISA
- Executive orders establish government expectations in this area
- Guidance does not align with current norms, in part, because it suggests to add vulnerabilities to the SBOM (this is NOT typically in an SBOM)
  - However, does not prevent use of NTIA or other methodologies
- To facilitate the use of SBOM management tools for critical infrastructure sectors and to ensure compliance with Executive Order 14028, hope to see that the elements of the SBOM are revised to align with NTIA’s publication “The Minimum Elements for a Software Bill of Materials” (July 12, 2021).

#3: Architectural Views

- Assessing and Documenting Architecture
  I. Implementation of Security Controls: consider recommended controls across the architecture
  II. Security Architecture Views: Documenting these views should include both diagrams and explanatory text.



The container diagram for the Internet Banking System.
Personal Banking Customer
[Person]
A customer of the bank, with personal bank accounts.
Visits bigbank.com/ib using [HTTPS]
Views account balances, and makes payments using
Views account balances, and makes payments using
Sends e-mails to
Web Application
Delivers the static content and the Internet banking single page application.
Delivers to the customer's web browser
Single-Page Application
Provides all of the Internet banking functionality to customers via their web browser.
Mobile App
Provides a limited subset of the Internet banking functionality to customers via their mobile device.
E-mail System
[Software System]
The internal Microsoft Exchange e-mail system.
Makes API calls to [JSON/HTTPS]
Makes API calls to [JSON/HTTPS]
Sends e-mail using [SMTP]
Database
Stores user registration information, hashed authentication credentials, access logs, etc.
Reads from and writes to [JDBC]
API Application
Provides Internet banking functionality via a JSON/HTTPS API.
Makes API calls to [XML/HTTPS]
Mainframe Banking System
[Software System]
Stores all of the core banking information about customers, accounts, transactions, etc.
Internet Banking System
[Software System]
Personal Banking Customer
E-mail System
Mobile App
Web Application
Single-Page Application
API Application
Mainframe Banking System
Database

#3: Architectural Views

- VIEWS: architecture information take the form of “views,”:
  - Global System View;
  - Multi-Patient Harm View;
  - Updateability/Patchability View; and
  - Security Use Case View(s).
  - Documenting these views should include both diagrams and explanatory text.
- **Interesting approach:** this should all be part of Threat Modeling. A large portion of the guidance is organized around these views, stressing its importance. Does state that they “can” be added to the threat model. We recommend these are part of threat modeling.

#4: Labeling Recommendations

"…inadequate cybersecurity controls may cause a device to be misbranded under section 502(f) of the FD&C Act because **its labeling does not bear adequate directions for use** or under section 502(j) of the FD&C Act because it **is dangerous to health when used in the manner recommended or suggested in the labeling**, among other possible violations." (lines 238-240)

Labeling is a transparency issue (line 193): Ways for lack of transparency to be issue:

- LACK OF ADVISORIES/DISCLOSURE: insufficient information pertaining to whether a device has undisclosed cybersecurity vulnerabilities or risks may be relevant to determining whether a device's safety or effectiveness could be degraded
- LACK OF LABELING ON CONFIGURATION AND UPDATES: user manuals that do not include sufficient information to explain how to securely configure or update the device may limit the ability of end users to appropriately manage and protect the device;
- LACK OF INTERFACE TRANSPARANCY: a failure to disclose all of the communication interfaces or third-party software could fail to convey potential sources of risks. (also aligns with FDA Interoperability guidance)

#5: SPDF: What is this now?

FDA describes an SPDF as "a set of processes that reduce the number and severity of vulnerabilities in products throughout the device lifecycle."

- The SPDF should comprise a device maker's security focused risk management efforts, as well as development of a robust security architecture of each of its devices and performing cybersecurity testing, such as definition of security requirements, threat mitigation, vulnerability testing, and penetration testing according to the draft guidance.

Key Takeaways:

- FDA is firmly stating that cybersecurity needs to be integrated into the quality system to meet Quality System Regulation (QSR) requirements
- Security is being tightly tied to safety concerns

#6: Security Objectives vs 80001-2-2

Does not align with ISO/IEC 80001-2-2 and its 19 Security Capabilities. Instead, it calls them “security objectives” and only lists a subset:

“Security Objectives:

1. Authenticity including integrity
2. Authorization
3. Availability
4. Confidentiality

Secure and timely updatability and patchability“

So if you use the 19 capabilities, you can align them with these objectives to harmonize your baseline expectations.

Want to see how these are met through:

- Security requirements
- Architecture
- Supply chain
- Implementation

#7: Security Risk Management

- NOTABLE: FDA is stating, clearly and unequivocally, that ISO 14971 and Security Risk Management are distinct. Throughout the document, the agency reiterates that the risk management work per ISO 14971 may reach a different and contrary conclusion and while these two types of activities are inherently related, they should be dealt with as distinct.

  - FDA recommends that device manufacturers conduct both a safety risk assessment per ISO 14971:2019 and a separate, accompanying security risk assessment to ensure a more comprehensive identification and management of patient safety risks

- System Level Considerations: the safety and security risks of each device should be assessed within the context of the larger system in which the device operates (line 293)

#7: Security Risk Management

- **Probability versus Likelihood:** FDA acknowledges that failures cannot be probability based:

- Effective security risk management also addresses that cybersecurity-related failures do not occur in a probabilistic manner where an assessment for the likelihood of occurrence for a particular risk could be estimated based on historical data or modeling.

- This non-probabilistic approach is not the fundamental approach described in safety risk management under ISO 14971:2019. Instead, security risk assessment processes focus on exploitability, or the ability to exploit vulnerabilities present within a device and/or system. (line 315-2170

#7: Security Risk Management

- Line 570: “These risks may include those introduced by device reliance on hospital networks, cloud infrastructure, or “other functions” (as defined in FDA’s guidance “Multiple Function Device Products: Policy and Considerations), for example.”

    - This is an important note and stresses the importance of carefully scoping the risk management and threat modeling activity. Medical devices are not considered a black box when part of a connected health system.

#8: List of Documents for Submission

FDA purposely did not include any list of submission documents. They want to you review what is asked for in the guidance in context with the content.

This proves challenging for the average regulatory professional.

Most other premarket guidance documents will provide a specific list of documents to ensure clarity. We will discuss this further in #10

#9: References to the QSR

You may notice a significant increase in the number of QSR and CFR references in the new draft.

This is not an accident

- QSR – 21 times
- CFR – 51 times

Increase reference to specific regulations is a reminder that the expectations outlined in this guidance are relevant to current quality system regulations, so you need to be prepared for any of this to be requested by FDA.

#10: What is expected in submission today?

Some notable elements:

- Threat models are needed. They are part of Security Risk Management
- SBOMs needed if they are provided to customers
- MDS2 forms are needed if they are provided to customers
- Security Risk Management Documentation: including your rationale for the selection of evaluation and acceptance criteria (CVSS, Qualitative, etc)
- Details on postmarket plan and activities
- Complex attack scenarios: How do you deal with them?

Plus, those items listed in the 2014 Premarket – pay attention to the focus on ensuring product is delivered "malware free"

#10: What is expected in submission even though it is draft?

Testing: not explicitly addressed in 2014 Premarket Guidance

- Types of testing includes but not limited to:
    - Verification – requirements based
    - Network Testing (load, latency tolerance/response, network failure, etc.)
    - Static and Dynamic Code Analysis
    - Vulnerability Scanning
    - Fuzz Testing (Malformed input)
    - Penetration testing – full report!
- Third-Party Testing

Michelle Jump
Chief Executive Officer
MedSec LLC
michellejump@medsec.com