James Graves

IVD Submissions Workshop: Cybersecurity: A Shared Responsibility

April 21, 2022

FDA'S REGULATORY REQUIREMENTS – WHAT YOU NEED TO INCLUDE IN YOUR PREMARKET SUBMISSIONS

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.

Cybersecurity Reviews

- "… software engineering is about *ensuring that certain things happen …*, **security is about ensuring that they don't**"[1]
- What **can** the device do or be made to do versus what it was **designed** to do?
- Past Performance ≠ Future Security
- "Who is ever going to do that?"

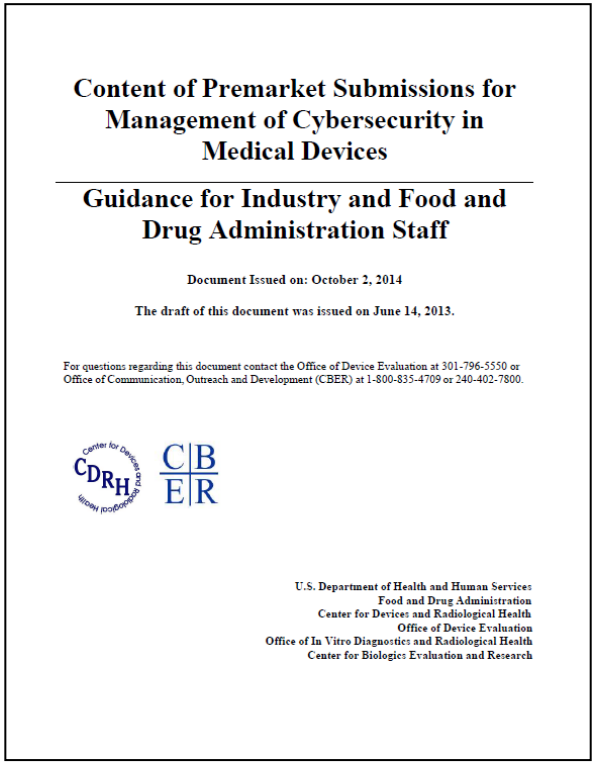
1. Anderson, Ross. "Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Edition" 2008.

Cybersecurity Reviews

- "… software engineering is about *ensuring that certain things happen …*, **security is about ensuring that they don't**"[1]
- What **can** the device do or be made to do versus what it was **designed** to do?
- Past Performance ≠ Future Security
- ~~"Who is ever going to do that?"~~

1. Anderson, Ross. "Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Edition" 2008.

FDA Cybersecurity Guidance



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

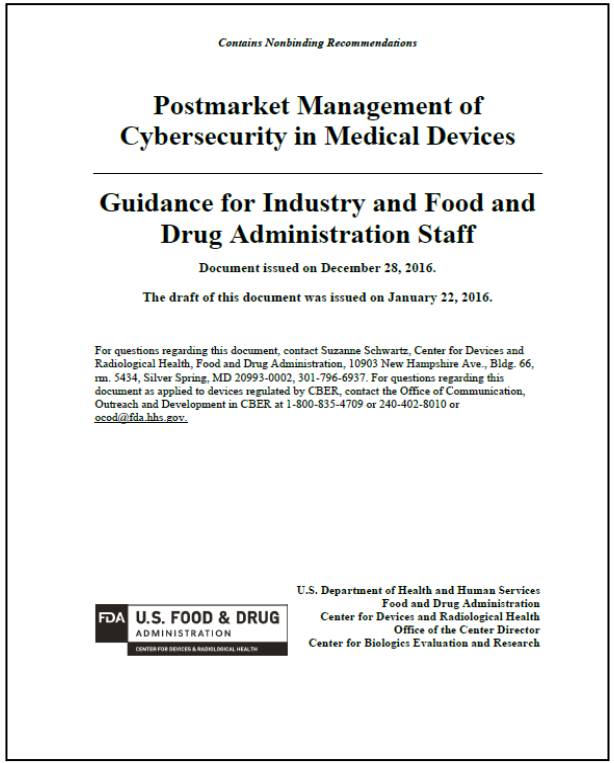
Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics 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.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

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

Does Cybersecurity Apply?

- Device is software, contains software, and/or contains any of these 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.)
- Cybersecurity added to Refuse to Accept Policy for 510(k) applications

Cybersecurity Reviews Today

- Risk Management
- Plan for Continuing Support
- Plan for Malware Free Shipping
- Labeling
- Testing

Identifying Risks and Mitigations

- Threat Modeling
- Assessment of Vulnerabilities from Third-Party Software
- Cybersecurity Risk Assessments
  - Assessment of impact of risk/vulnerability on safety and effectiveness of the medical device based on:
    - Severity of Patient Harm (if the vulnerability were to be exploited)
    - Exploitability (different assessment from probability of occurrence – non-deterministic)
  - Multi-Patient Risks

Plan for Continuing Support

- Details how a manufacturer will monitor and maintain cybersecurity once the device is marketed.
- Common Elements
  - Personnel Responsible
  - Sources for Identifying Vulnerabilities (Complaints, Researchers, NIST NVD, etc.)
  - Retesting and Regulatory Submission Criteria (can be leveraged from QS)
  - Patching Capability and Update Process
  - Frequency of Assessment

Malware Free Shipping

- Manufacturing controls to ensure malware is not introduced into software/device prior to shipment and/or update
- Software update/delivery mechanism and associated security controls to ensure the software cannot be compromised in delivery to device/system
  - USB updates
  - Remote updates (over-the-air)
  - Cloud software updates

Labeling

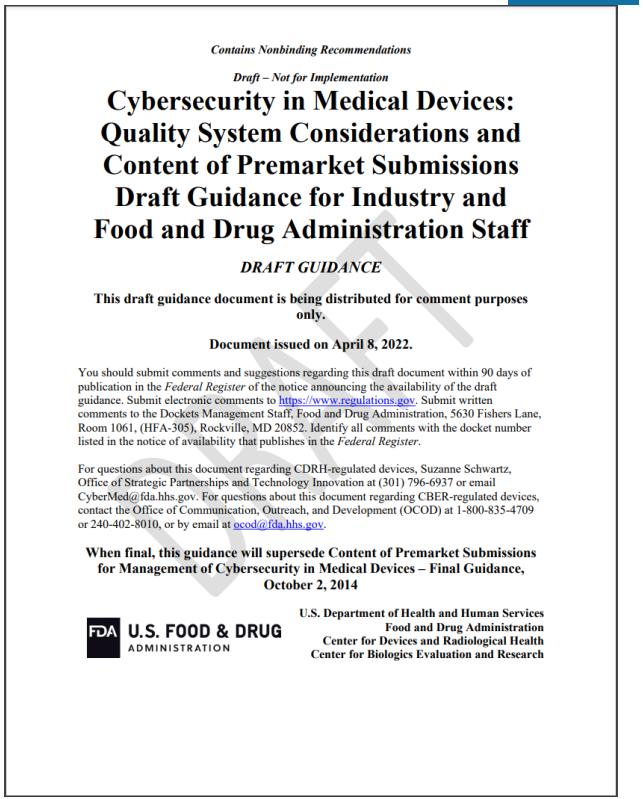
- Instructions to ensure the safe and effective use of the device
  - Interfaces (especially network interfaces) and functionality
  - Security controls user interacts with (e.g. password, software update mechanisms, etc.)
  - Manufacturer Disclosure Statement for Medical Device Security
    - Also called MDS2 or MDS^2 (if provided to customers)
  - Software Bill of Materials (SBOM) (if provided to customers)
    - Useful in verifying completeness of COTS/SOUP assessment
  - Logging capabilities and forensic log capture

Testing

- Not explicitly addressed in 2014 Premarket Guidance but is needed to demonstrate effectiveness of controls in security environment
- 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
- Third-Party Testing

Premarket Guidance: Draft 2022

- Currently available for comment (comment by July 7, 2022)
- Revisions based on comments received and additional learnings
- Secure Product Development Framework



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

James Graves
Biomedical Engineer
Division of Radiological Health

Digital Health Center of Excellence Program Director
OPEQ Cybersecurity Focal Point Program
Matthew.Hazelett@fda.hhs.gov