Software and Instrumentation Review and Cybersecurity Considerations

Lisa Simone, Ph.D.
Division of Emerging and Transfusion Transmitted Diseases
Office of Blood Research and Review
CBER

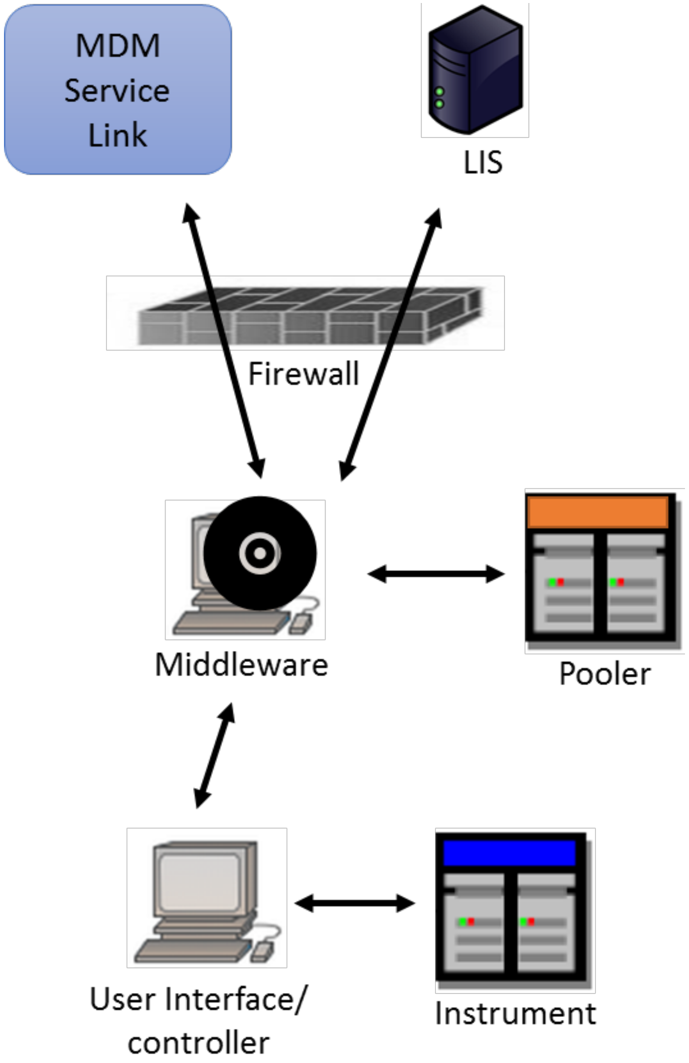
July 15, 2019

Presentation Outline

- Systems level approach to review
- Baseline topics for a risk-based software and instrumentation review
- Newer topics for challenges in the use environment
  - Interoperability
  - Cybersecurity
- Updates for Premarket Cybersecurity Guidance (in progress)

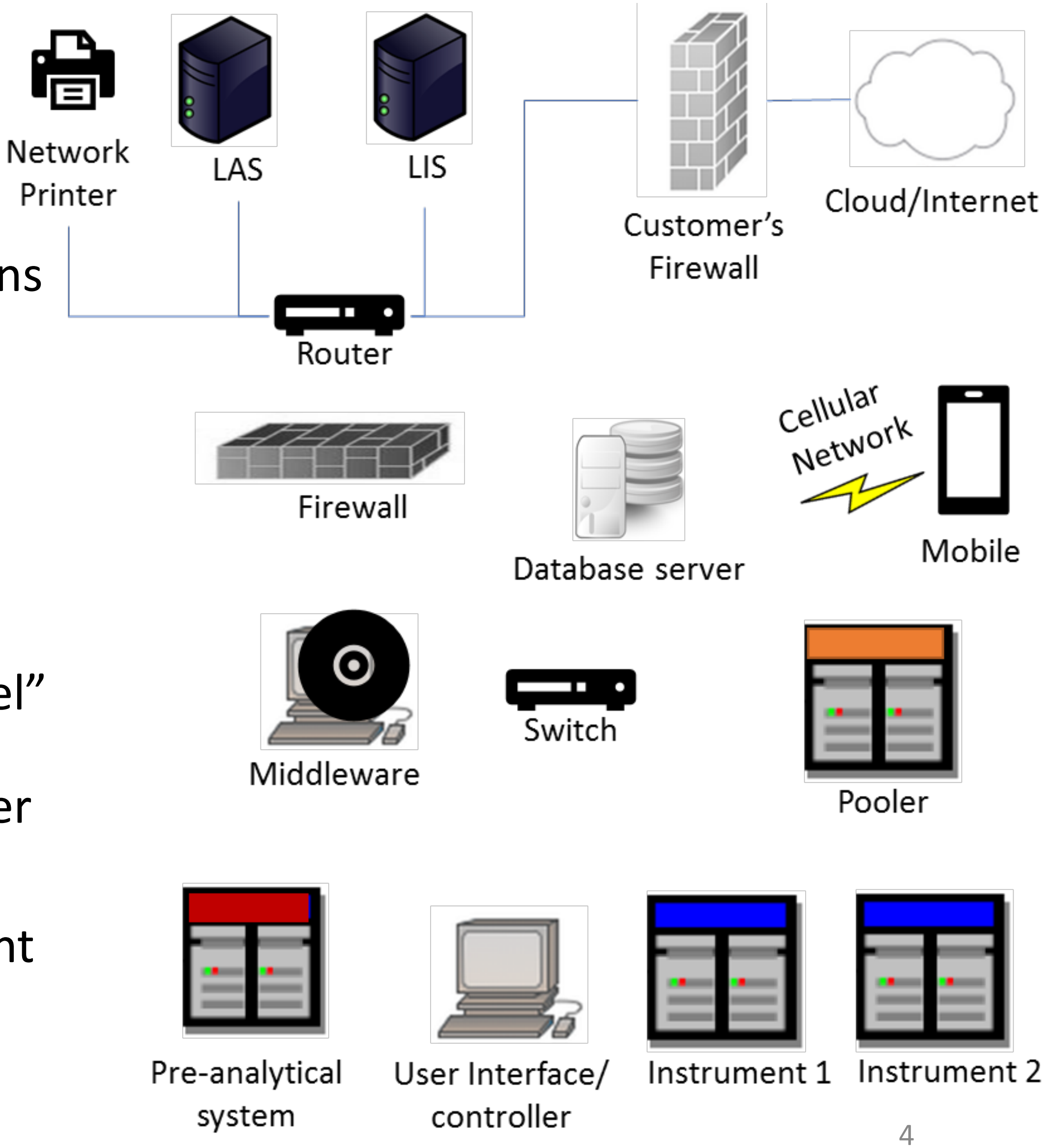
Overview of Device Configurations (1)

- Systems often include several parts to meet the intended use
- Different configurations, different workflows
- May interface to different networks
- Some systems are straightforward - all parts from the same Medical Device Manufacturer (MDM)

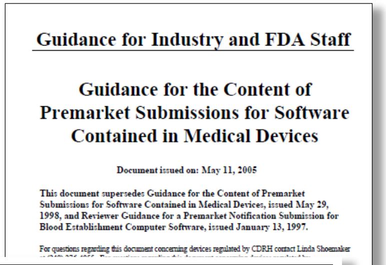


Overview of Device Configurations (2)

- Other systems are more complex, with multiple parts and connections
- Regulatory requirements may be different for each part
- Premarket review considers how each contributes to the risk of the overall system
- For review, additional “system level” documentation may be needed to demonstrate how all parts together are reasonably safe and effective
- Interoperability becomes important



Baseline for Software and Instrumentation Review



Guidance for Industry and FDA Staff

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Document issued on: May 11, 2005

This document supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, issued May 29, 1998, and Reviewer Guidance for a Premarket Notification Submission for Blood Establishment Computer Software, issued January 13, 1997.

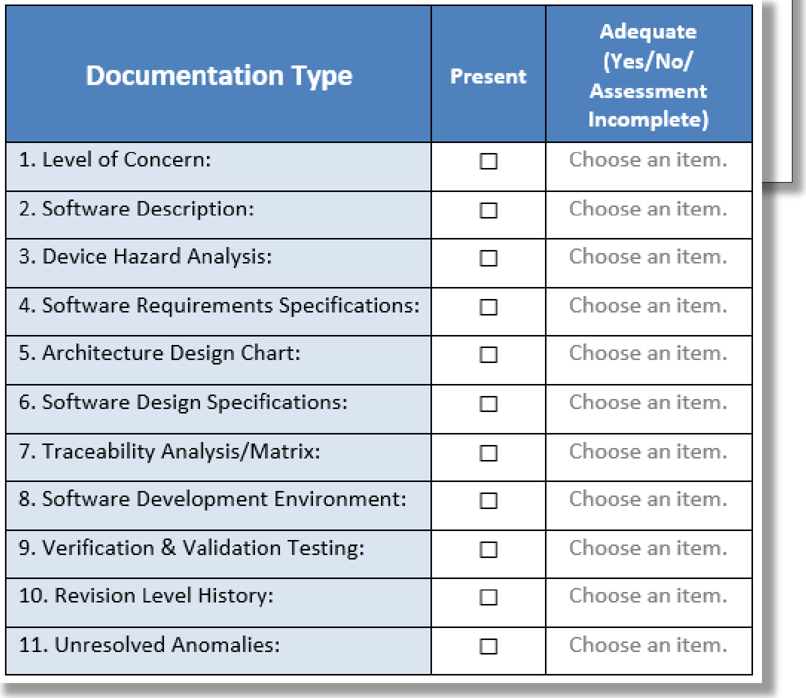
For questions regarding this document concerning devices regulated by CDRH contact Linda Shoemaker

Documentation for review outlined in many guidance documents

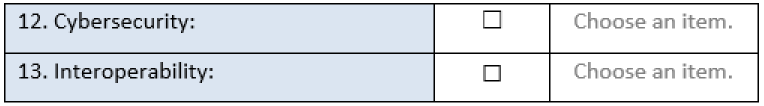
- Most familiar: "*Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*"

Because devices operate in increasingly complex use environments:

- Cybersecurity guidance (premarket 2014 and postmarket 2016)
- Interoperability guidance (2017)



Documentation Type	Present	Adequate (Yes/No/ Assessment Incomplete)
1. Level of Concern:	□	Choose an item.
2. Software Description:	□	Choose an item.
3. Device Hazard Analysis:	□	Choose an item.
4. Software Requirements Specifications:	□	Choose an item.
5. Architecture Design Chart:	□	Choose an item.
6. Software Design Specifications:	□	Choose an item.
7. Traceability Analysis/Matrix:	□	Choose an item.
8. Software Development Environment:	□	Choose an item.
9. Verification & Validation Testing:	□	Choose an item.
10. Revision Level History:	□	Choose an item.
11. Unresolved Anomalies:	□	Choose an item.



12. Cybersecurity:	□	Choose an item.
13. Interoperability:	□	Choose an item.

"Guidance for Industry and FDA Staff - Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" https://www.fda.gov/media/73065/download.
"Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff" https://www.fda.gov/media/86174/download.
"Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff" https://www.fda.gov/media/95862/download.
"Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices" https://www.fda.gov/media/95636/download.

Issues with Submissions

Documentation

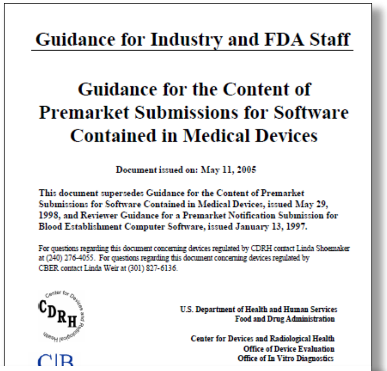
Issues	Impact
Cover letter does not describe true reason for the submission	Hard to identify specific changes that are focus the review
Documentation difficult to search, hyperlinks missing or incorrect	Check links and PDF creation to allow least burdensome review. Use helpful filenames.
Complex tables rendered into microscopic PDF font sizes	Review PDFs for readability

How the software guidance documentation is used in review

Review goal: focus on what can go wrong in the system, and identify what has been done to reduce those risks to acceptable levels

- Not a “checklist” review – focus on risks
- Establish reasonable assurance of safety and effectiveness
- Reduce burden for applicant and reviewer

The documentation should support a risk-based review



Guidance for Industry and FDA Staff

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

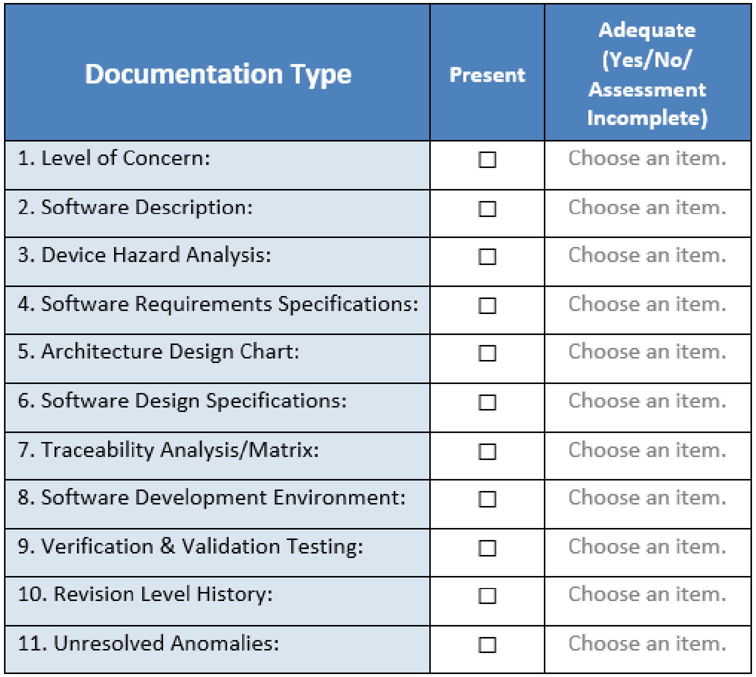
Document issued on: May 11, 2005

This document supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, issued May 29, 1998, and Reviewer Guidance for a Premarket Notification Submission for Blood Establishment Computer Software, issued January 13, 1997.

For questions regarding this document concerning devices regulated by CDRH contact Linda Shoemaker at (240) 276-4055. For questions regarding this document concerning devices regulated by CBER contact Linda Weir at (301) 827-6136.

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



Documentation Type	Present	Adequate (Yes/No/ Assessment Incomplete)
1. Level of Concern:	□	Choose an item.
2. Software Description:	□	Choose an item.
3. Device Hazard Analysis:	□	Choose an item.
4. Software Requirements Specifications:	□	Choose an item.
5. Architecture Design Chart:	□	Choose an item.
6. Software Design Specifications:	□	Choose an item.
7. Traceability Analysis/Matrix:	□	Choose an item.
8. Software Development Environment:	□	Choose an item.
9. Verification & Validation Testing:	□	Choose an item.
10. Revision Level History:	□	Choose an item.
11. Unresolved Anomalies:	□	Choose an item.

Risk-Based Review (1)

1. Is the system doing the right thing? →
   - Does it satisfy its medical purpose?

2. Is the system *not* doing the *wrong* thing? →
   - Does it detect and prevent error situations that could cause incorrect operation?

This is a critical aspect of a risk-based review

Risk-Based Review (2)

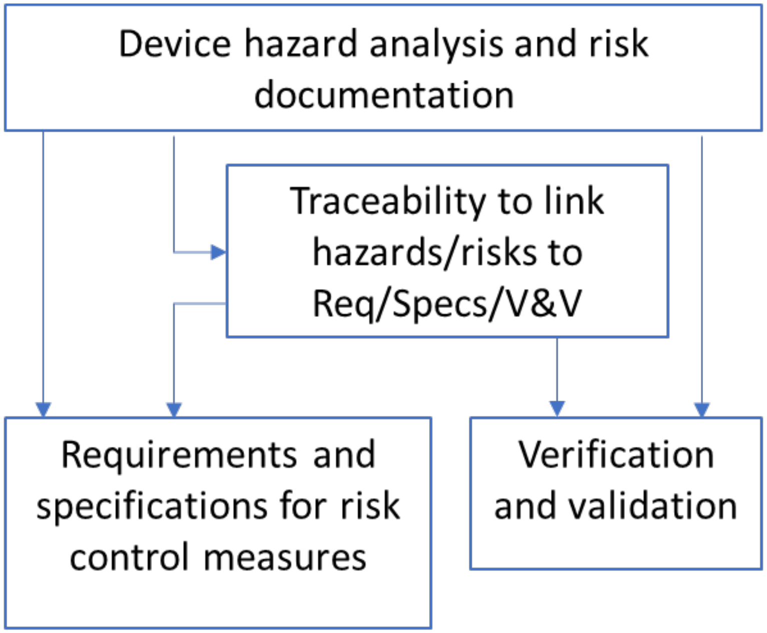
Approach	Documentation Referenced
1. Learn about system/device What does the device do?	• Intended Use • Software Description • Device Description in submission • Manuals, etc.
How does the device do it? Technology behind the operation	• Usually spread throughout the submission, but focuses on: • Architecture, • Requirements, • Specifications, and • Many non-software sections

Risk-Based Review (3)

Questions Asked

Documentation Referenced

2. Risk of harm
   - Identify issues that have higher estimates of risk (focus on the harms that can occur)
   - Identify specific risk control measures that reduce the risk of harm
   - Identify testing to demonstrate risk control measures verified
   - Review higher residual risks



Device hazard analysis and risk documentation

Traceability to link hazards/risks to Req/Specs/V&V

Requirements and specifications for risk control measures

Verification and validation

3. Other sources of risk

Unresolved anomalies (open issues)
Revision history information (changes made)

Issues with Submissions

Device Hazard Analysis

Issues	Impact
Risk management process not provided or explained	Can’t evaluate if residual risks are acceptable. Align with industry standard process.
Estimations of risk prior to risk control/mitigation not provided	Can’t identify which controls are the most important in reducing risk
Clear trace between individual risk control measures and their verification test missing (incomplete traceability)	Can’t link risk controls to requirements and testing to determine if a risk control measure is reasonable and is verified to reduce risk
Risk analysis limited to only some parts of the overall system	Can’t draw conclusions about safety and effectiveness of entire system. Provide system level analysis.
Impact of any hardware changes from previous submissions or during trials is not discussed	Device HA is not limited to software hazards

Issues with Submissions

Assay Hazard Analysis

Issues	Impact
Specific assay-related hazards/harms not included	Can't tell if analysis considered assay-specific hazards and individual hazardous situations (e.g., typical, worst case)
MAUDE adverse event data used as an estimate of probability	Helps identify hazard causes and contributing factors. It shouldn't be used to estimate probabilities (data quality issues, underreporting).
Risk acceptability criteria not provided, or individual benefit/risk justifications missing (if needed)	Can't evaluate if residual risks are acceptable. Benefit/risk determinations for individual risks may be necessary.
Factors that are outside the manufacturer's control are used to reduce estimates of risk in the device hazard analysis	Factors such as viral inactivation or presence of disease-treating drugs inform benefit/risk discussions. These are not device risk control measures.
Software was upgraded during preclinical/clinical studies	Changes are possible if risk assessment shows no impact on the data previously collected (use pre-sub pathway for questions)

Issues with Submissions

Testing

Issues	Impact
Test plans/protocols missing	May needed to evaluate type of testing performed, esp. for higher risks
Missing verification of information for safety	Risk reduction that relies on labeling should be verified (e.g., usability tests)
Failed tests not explained/justified	Can't determine impact of failed tests on safety and effectiveness. Provide assessment.

Issues with Submissions

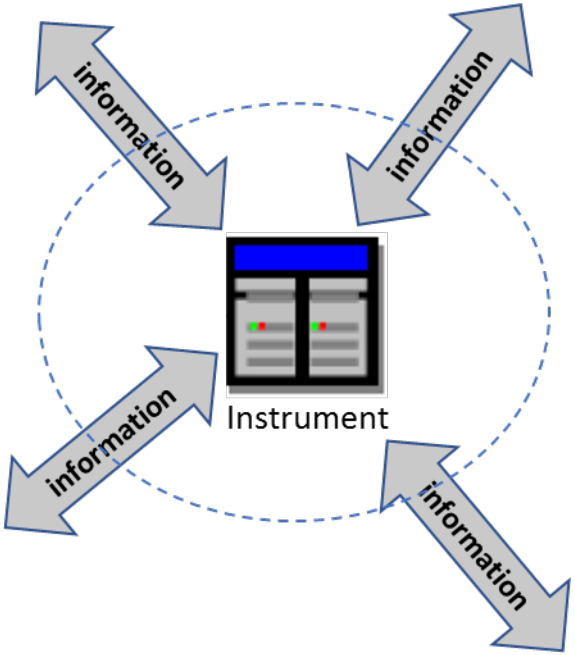
Other Issues

Issues	Impact
Unresolved anomalies don't include impact on safety and effectiveness, operator usage and human factors	Can't determine the impact of leaving defects unresolved in marketed system. Provide justification.
Unclear how end user notified of anomaly-related risks/workarounds	Can't assess how residual risks are disclosed to user. Include traces to labeling where risks are disclosed.
Full documentation not provided for standalone software/SaMD	Review must consider risks related to use of all software in the system

Operating in the Use Environment: Interoperability and Cybersecurity

Interoperability: Two or more products, technologies or systems exchanging and using information

- Example information exchanged:
  - patient data
  - assay information
  - instrument data
  - command and control over other devices
  - mobile notifications, etc.
- Example purposes:
  - support intended use
  - receive software updates
  - perform backup/restore
  - service/maintenance, etc.
- Connectivity leads to increased risks

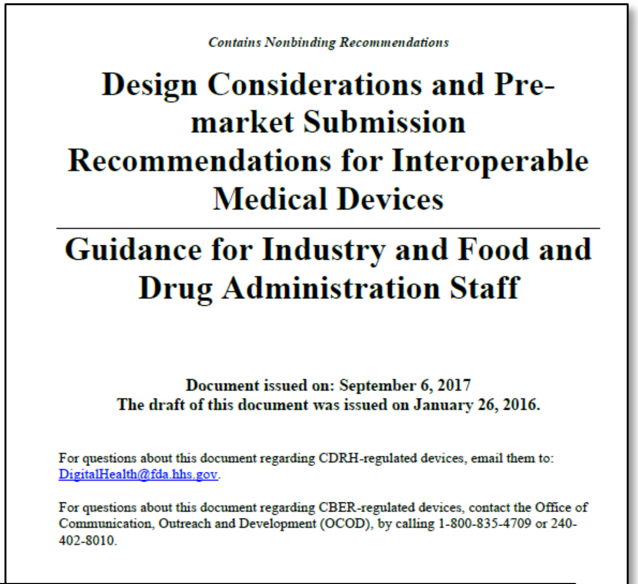


The Cybersecurity Environment

- Software in connected medical devices is vulnerable to threats
- Cybersecurity incidents can directly impact medical devices or networked operations
- When vulnerabilities are not addressed, malware might enter and spread through user, lab, hospital/healthcare facility networks
- Compromise of data confidentiality, integrity, and availability may lead to patient harm, through:
  - Compromise of critical device functionality
  - Delay in diagnosis/treatment intervention

Interoperability Guidance:

- List on externally-facing electronic interfaces (EIs)
  - Purpose, role and anticipated users
  - Impact on device performance
  - How the interface is used, and limitations
- Risk analysis including security-related issues
- V&V under normal and abnormal conditions that are reasonably likely to occur
- Information in Labeling



Contains Nonbinding Recommendations

Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices

Guidance for Industry and Food and Drug Administration Staff

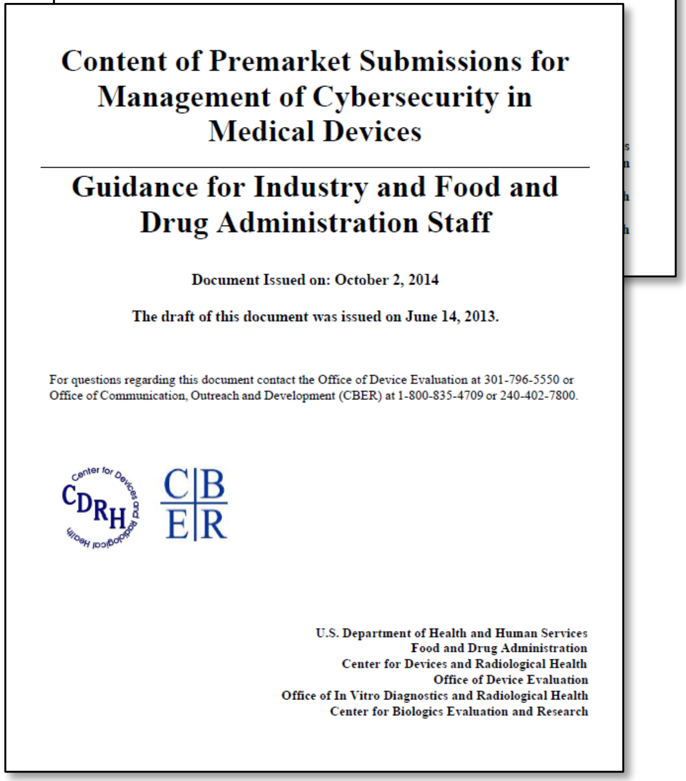
Document issued on: September 6, 2017
The draft of this document was issued on January 26, 2016.

For questions about this document regarding CDRH-regulated devices, email them to: DigitalHealth@fda.hhs.gov.

For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 240-402-8010.

Cybersecurity Guidance:

- Hazard analysis related to intentional and unintentional cybersecurity risk
- Traceability matrix linking cybersecurity risks to controls
- Summary of plan to provide validated software updates and patches
- Summary of controls to assure medical device will maintain its integrity throughout design and release
- Recommended cybersecurity controls (e.g., antivirus, firewall)



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

Issues with Submissions

Interoperability

Issues	Impact
Assumption that interoperability guidance does not apply	Guidance drives risk identification for all functionality used as part of the system. Analysis should include unintentional misuse and malicious use.
List of externally-facing electronic interfaces (EIs) not provided, although hardware may list multiple USBs, network ports, etc.	Prevents clear picture of connectivity and risks associated with connected functionality. List/discuss EIs individually.
Connected functionality mentioned without reference to EIs, protocols, protections	Hinders review of risk and cybersecurity considerations. Include requested information.

Issues with Submissions

Cybersecurity

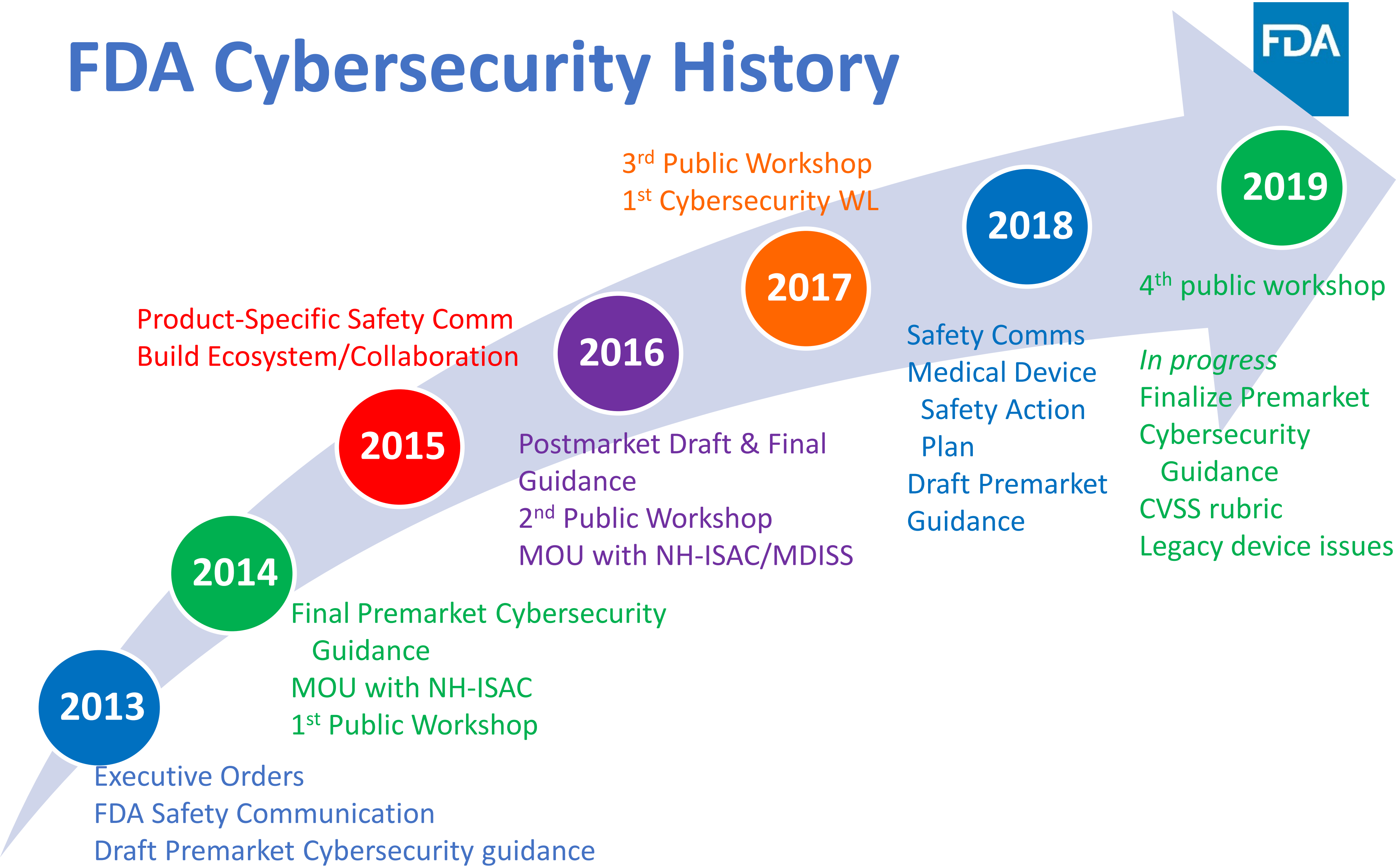
Issues

- Diagrams of system components not provided (e.g., network diagrams, data flow, etc.)
- Cybersecurity controls not linked to specific cybersecurity risks
- Cybersecurity is treated like a silo
- Not assuming the worse case scenario for a security-related risk
- Not hardening the system to prevent access of unused ports

Issues

- Not disclosing residual risks to users to inform their risk management activities (shared responsibility)
- Not considering End of Support dates for operating systems
- Not considering the security risks associated with use of off-the-shelf (OTS) software, and therefore not validating OTS software for security, in addition to safety and effectiveness

FDA Cybersecurity History



2013

Executive Orders
FDA Safety Communication
Draft Premarket Cybersecurity guidance
Began Coordination with DHS
Recognized Standards
Established the Cybersecurity Working Group (CSWG)
Recall of TNS-listener

2014

Final Premarket Cybersecurity Guidance
MOU with NH-ISAC
1st Public Workshop

2015

Product-Specific Safety Comm
Build Ecosystem/Collaboration

2016

Postmarket Draft & Final Guidance
2nd Public Workshop
MOU with NH-ISAC/MDISS

2017

3rd Public Workshop
1st Cybersecurity WL

2018

Safety Comms
Medical Device Safety Action Plan
Draft Premarket Guidance

2019

4th public workshop

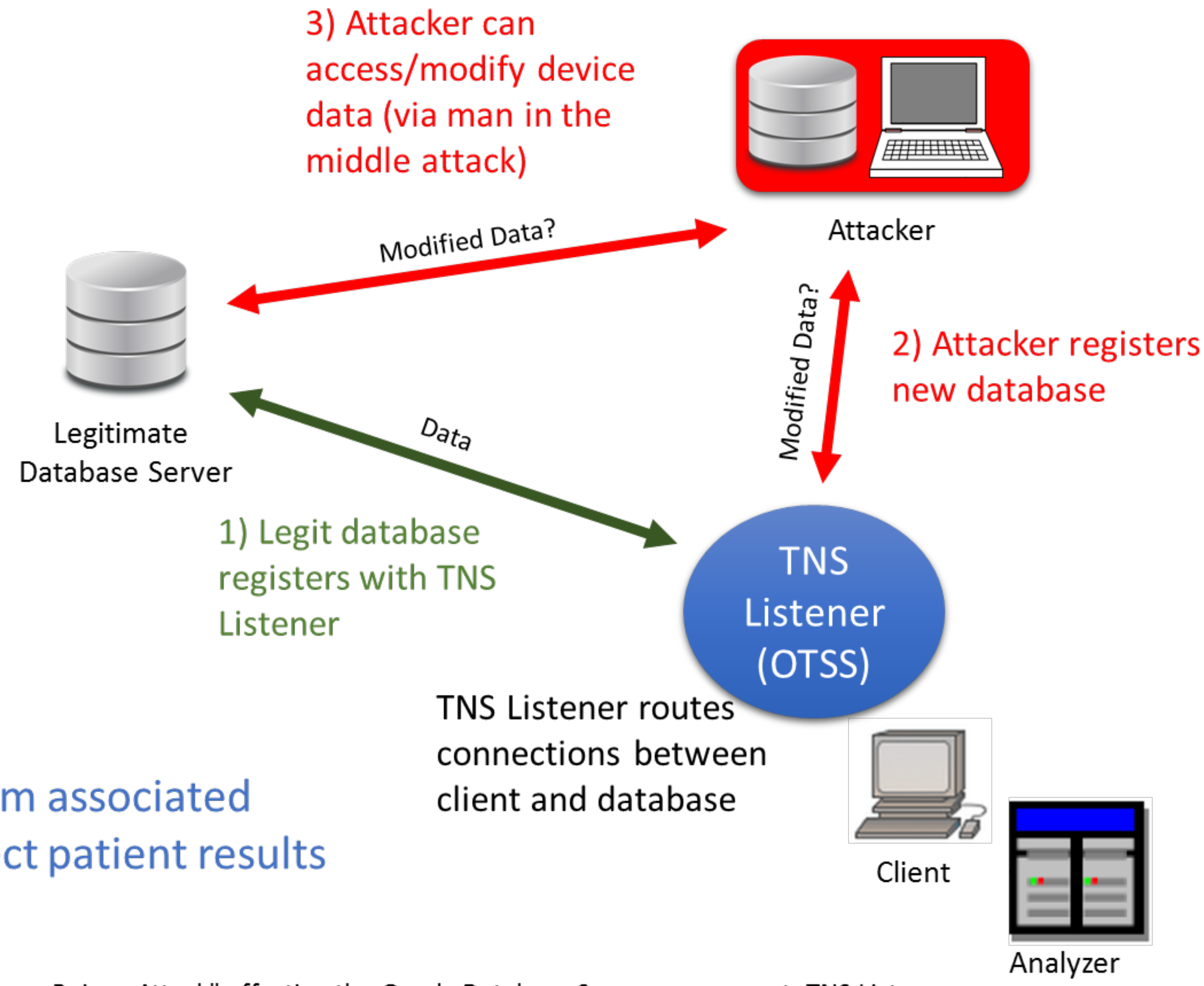
In progress
Finalize Premarket Cybersecurity Guidance
CVSS rubric
Legacy device issues

Vulnerabilities and Medical Devices

- FDA's thinking has evolved based on external security events and our review of documentation provided
- Recent issues drive FDA's actions
  - Hackable infusion pump that may over- or under-infuse drugs
  - Implanted cardiac devices that might stop working or work incorrectly
- Exploits might not target medical devices directly
  - WannaCry impacted those who hadn't installed a security update for Windows XP (legacy issue)
- Issues on the horizon
  - Ransomware in the short term
  - Attacks that influence the physics of sensors to change their input and outputs; e.g., using radio waves, acoustics
  - Tampering of medical records and trustworthiness of chart data used to treat and diagnose patients

Kevin Fu: https://www.aami.org/productspublications/articledetail.aspx?ItemNumber=5730

Recalled Device for Vulnerability in Off-the-Shelf Software



3) Attacker can access/modify device data (via man in the middle attack)

2) Attacker registers new database

1) Legit database registers with TNS Listener

TNS Listener routes connections between client and database

Possible harm associated with incorrect patient results

CVE-2012-1675, "TNS Listener Poison Attack" affecting the Oracle Database Server component, TNS Listener

Updated Cybersecurity Premarket Guidance: What's New

- Because medical device cybersecurity continues to evolve, new guidance is needed
- Designing trustworthy devices – security spans the entire product lifecycle
  - Integrating threat modeling
  - Secure development lifecycle
  - Considering "exploitability" of a vulnerability rather than estimating probabilities
  - Software Bill of Materials
- Shifting the mindset to scenarios in the use environment beyond "intended use"
- Engage in proactive behavior and information sharing
- Preventing multi-patient (i.e., scaled) attacks

Parting Thoughts for Software and Instrumentation Review

Documentation Needs

Play your part in a least burdensome review

- Review applicable guidance documents for what to provide
- Provide great risk analysis to guide a risk-based review
- Ensure V&V covers higher risks at a minimum
- Anticipate reviewer questions: proactively explain any discrepancies, failed tests, anomalies, use of multiple software versions for testing, etc.

Our Documentation Asks

- Documentation must support review of the entire system for
  - safety and effectiveness, and
  - security
- If system contains elements from more than one manufacturer, agreements might be necessary to allow FDA to review the necessary documentation
- When in doubt, use FDA's presubmission pathway for advice

Thank you!

Lisa Simone
lisa.simone@fda.hhs.gov

Guidance Reference List

The following is a list of the most common guidances considered when designing medical devices and for establishing documentation to support premarket reviews. This is not an exhaustive list.

- "Guidance for Industry and FDA Staff - Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices," issued May 11, 2005 and available at https://www.fda.gov/media/73065/download.
- "Guidance for Industry and FDA Staff: "Assay Migration Studies for In Vitro Diagnostic Devices," issued April 25, 2013 and available at https://www.fda.gov/media/73669/download.
- "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff," issued October 2, 2014 and available at https://www.fda.gov/media/86174/download.
- "Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," issued December 28, 2016 and available at https://www.fda.gov/media/95862/download.
- "Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices," issued September 9, 1999 and available at https://www.fda.gov/media/72154/download.
- "General Principles of Software Validation; Final Guidance for Industry and FDA Staff," issued January 11, 2002 and available at https://www.fda.gov/media/73141/download.
- "Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," issued January 14, 2005 and available at https://www.fda.gov/media/72154/download.
- "Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices," issued September 5, 2017 and available at https://www.fda.gov/media/95636/download.
- "Radio Frequency Wireless Technology in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," issued August 14, 2013 and available at https://www.fda.gov/media/71975/download.
- "Design Control Guidance for Medical Device Manufacturers," issued March 11, 1997 and available at https://www.fda.gov/media/116573/download.

FDA Guidance document search: https://www.fda.gov/regulatory-information/search-fda-guidance-documents

Cybersecurity References

- FDA's Website on Cybersecurity: https://www.fda.gov/medical-devices/digital-health/cybersecurity
    - Mitigating Cybersecurity Risks
    - Cybersecurity Guidelines
    - Cybersecurity Safety Communications
    - Reporting Cybersecurity Issues
    - MOUs on Cybersecurity in Medical Devices
    - Workshops and Webinars on Cybersecurity
    - Other Collaborations on Cybersecurity
    - Cybersecurity in the News
- Medical Device Safety Action Plan (April 2018): https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health
- AAMI BI&T: The Evolving State of Medical Device Cybersecurity March/April 2018: https://www.aami-bit.org/doi/full/10.2345/0899-8205-52.2.103
- Perspective piece in American Heart Association Journal 'Circulation' (Sept 2018:) https://www.ahajournals.org/doi/10.1161/CIRCULATIONAHA.118.035021
- Report on Advancing Coordinated Vulnerability Disclosure – MDIC publication (Oct 2018): http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf
- Suzanne B. Schwartz, MD, MBAFDA, Center for Devices and Radiological Health, USENIX 2018, Baltimore Maryland, Aug 17, 2018
- Seth D Carmody, PHD, HCISPP, CDRH / FDA, International Council on Systems Engineering Conference, May 1, 2019