Cybersecurity and Successful Premarket Review

FDA Small Business Regulatory Education for Industry (REdI)

Sliver Spring, MD

August 27, 2020

Lisa Simone

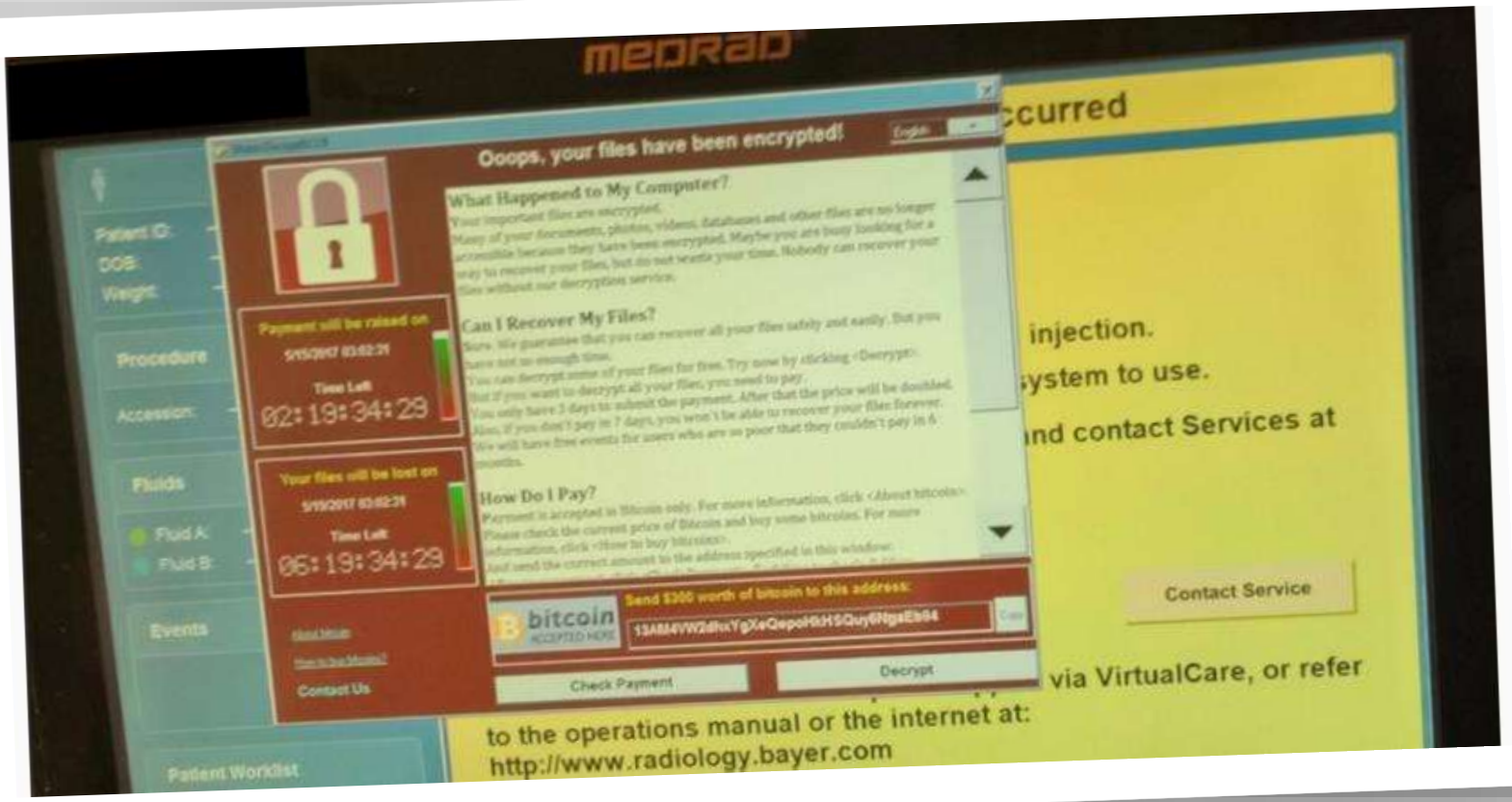
Cybersecurity Program Manager

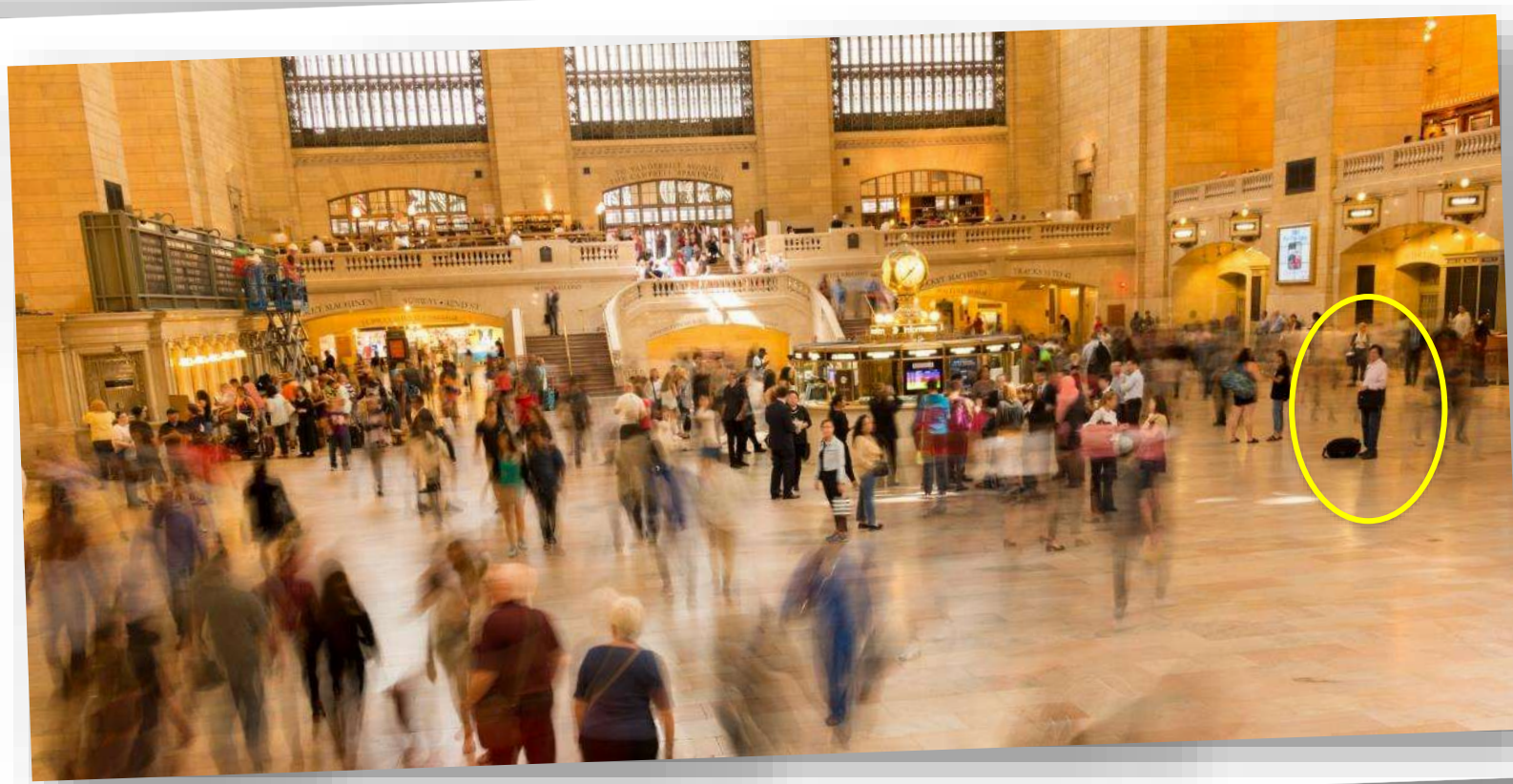
All Hazards Response and Cybersecurity

Office of Strategic Partnerships and Technology Innovation

Center for Devices and Radiological Health

U.S. Food and Drug Administration


MEDRAD
Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
Time Left
02:19:34:29
Your files will be lost on
Time Left
06:19:34:29
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt
Patient ID:
DOB:
Weight:
Procedure
Accession:
Fluids
Fluid A:
Fluid B:
Events
Patient Worklist
ccurred
injection.
system to use.
nd contact Services at
Contact Service
via VirtualCare, or refer
to the operations manual or the internet at:
http://www.radiology.bayer.com



What is the real use environment

Do you need to consider cybersecurity?

- [ ] Communicate with other devices?
- [ ] Current or potential future network connection?
- [ ] Wireless communication?
- [ ] USB port or physical media access?
- [ ] Remote software downloads (patching, upgrades)?
- [ ] Cloud storage or cloud services

Safety Risks vs. Cybersecurity Risks

Is the system doing the right thing? …

… Is this system **NOT** doing the **WRONG** thing?

Past Performance  Future Security

But, but, but … “Who is ever going to do that?”

Some Level-Setting

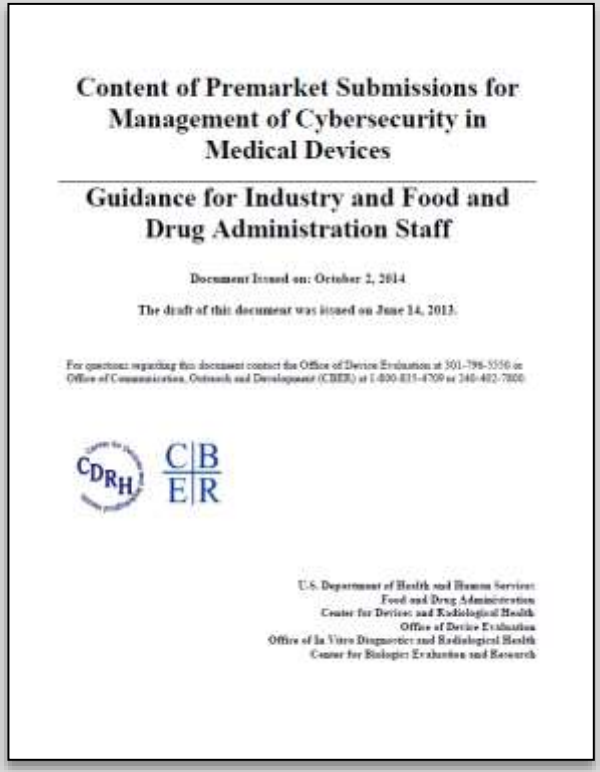
- A vulnerability is a weakness
- A threat is a circumstance/event that can adversely impact the device
  - Threats exercise vulnerabilities
  - Exploitability is the feasibility or ease by which a vulnerability can be exploited by a threat
- Method to reduce risk: risk control measures or risk mitigations
- Cybersecurity controls “control” cybersecurity risk

Learning Objectives

- Explain the focus of FDA's updated guidance
- Describe major objectives of a cybersecurity premarket review
- List testing that can demonstrate cybersecurity controls are effective
- List common issues that can prevent a successful premarket submission outcome

The Focus of FDA's Updated Guidance

FDA Cybersecurity Guidance



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

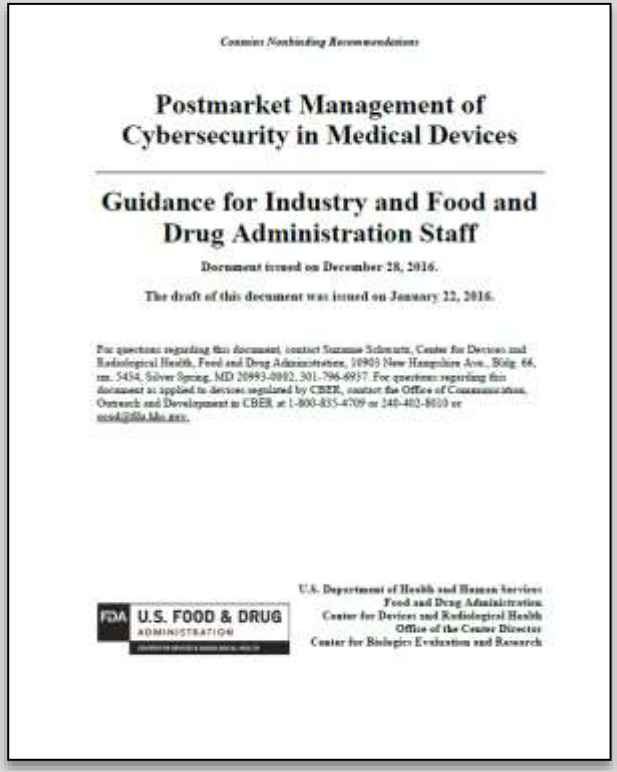
Guidance for Industry and Food and Drug Administration Staff

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. 5454, 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

Cybersecurity Reviews Components

Risk Management

Plan for Continuing Support

Plan for Malware Free Shipping

Labeling

Interoperability

Pain Points with 2014 Guidance

- Risks throughout product lifecycle not considered
- Missing information about software
- Insufficient security built into design
- Insufficient testing of security controls
- Insufficient information to users to manage risks
- Insufficient infrastructure to rapidly address security concerns

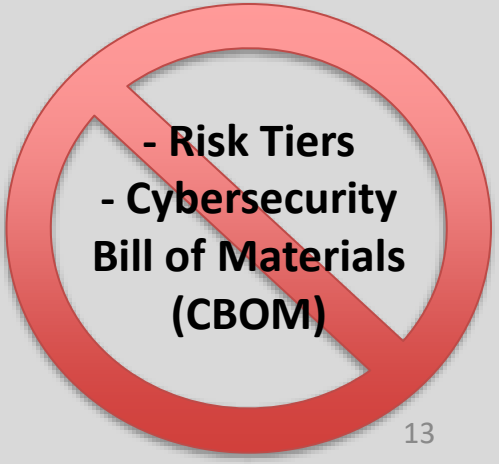
Premarket Guidance: Draft 2018

- Security is safety
- Security relies on the entire system
- Secure design = resilient devices

- Better aligns with a Secure Product Development Framework (SPDF); e.g.,
  - Medical Device and Health IT Joint Security Plan (JSP)
  - ANSI/ISA 62443-4-1 Security for industrial automation and control systems

Premarket Guidance Update

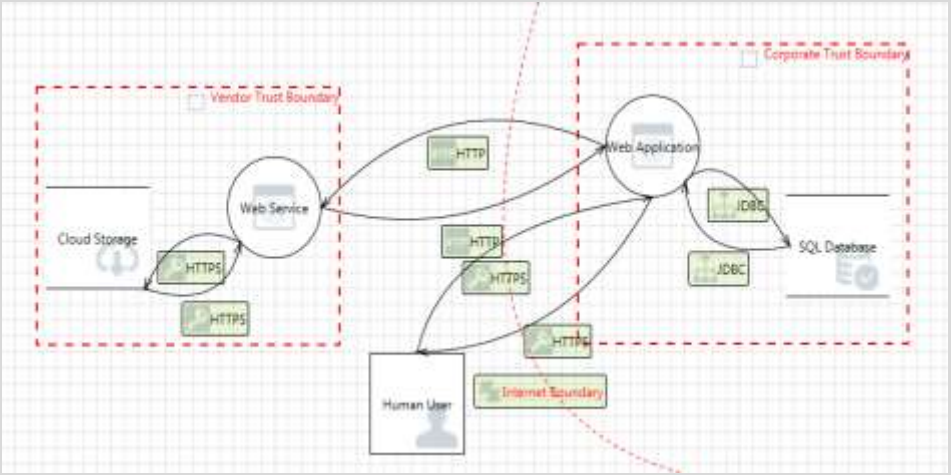
- Risk Management throughout the lifecycle
- Security Architecture Documentation
- Security Testing
- Transparency
- Qsub for feedback on proposed implementations



Cybersecurity Premarket Review

Risk Management

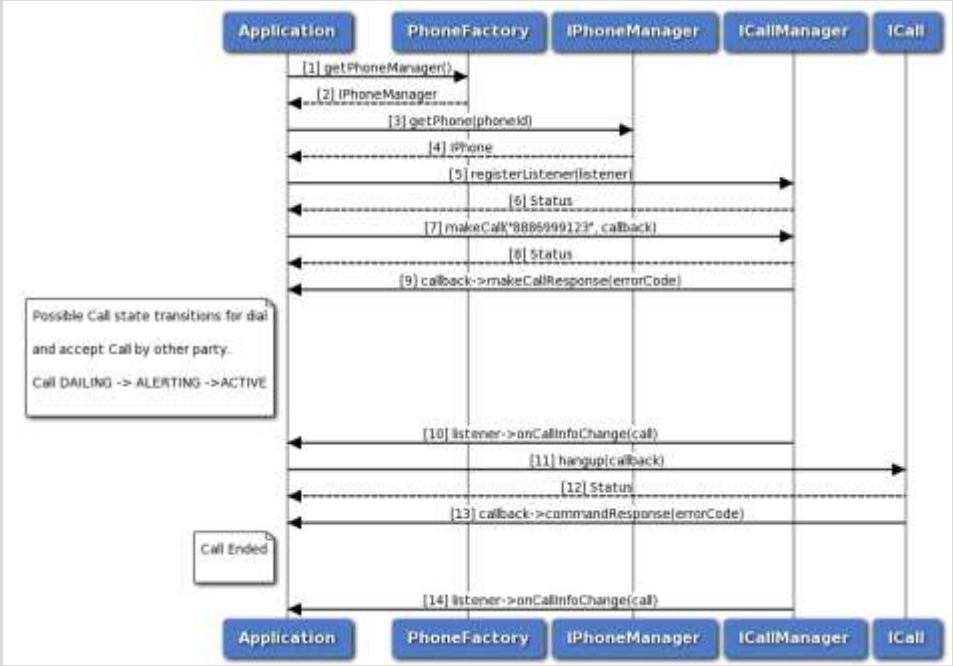
- Threat Modeling: identifying threats and defining countermeasures
- Include risks in supply chain, manufacturing, release, maintenance, etc.
- Consider larger system



Risk Management

Threat Modeling

- Various Methodologies
  - STRIDE, Kill Chain, MITRE ATT&CK, Attack Trees, etc.
- Outputs
  - Vulnerabilities and Controls



Risk Management

Assessing Cybersecurity Risks

Assess impact of vulnerability on safety and essential performance of the medical device based on:

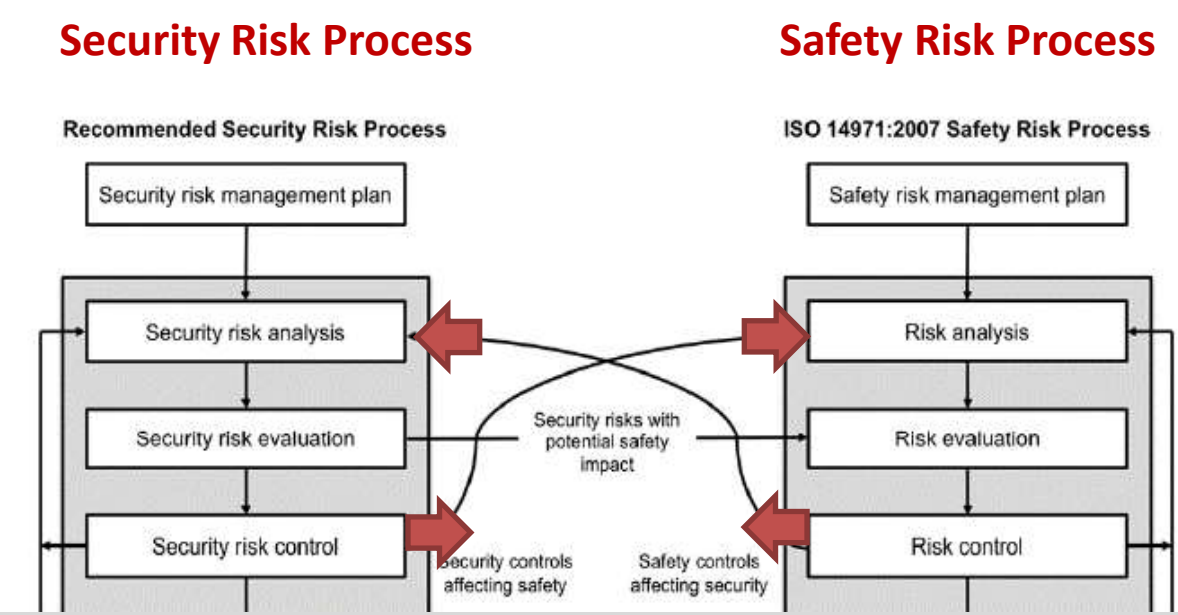
Severity of Patient Harm:	If vulnerability were exploited
Exploitability:	Different from likelihood, non-deterministic assessment

CVSS: framework of characteristics and severity of software vulnerabilities

Assessing Cybersecurity Risks

Tie together security and safety risk assessments

Some security risk assessments may fill both functions



AAMI TIR 57: 2016 Principles for medical device security – Risk management

Software Bill of Materials (SBOM)

- Manufacturer-developed and third-party
- SBOM aids management of cybersecurity risks
- Assess risks using vulnerability database
  - example: NIST National Vulnerability Database

See FDAs Guidance: OTS Networked Cybersecurity Guidance, OTS Software in Medical Devices

Scope of Documentation

- Addresses larger system context
- Describes end-to-end connections/ communications
- Risk tables show end-to-end how mitigations address risks

Show us your Defense in Depth!

Interoperability

- Align interoperability/cybersecurity concerns
- Explore all externally-facing Electronic Interfaces (EIs)
  - Active?
  - What's it used for?
  - Hazardous situations explored?
  - Testing adequate based on risk assessment?
  - Information in Labeling?

See FDA's 2017 Guidance, Interoperable Medical Devices

Transparency

- Continuing Support
  - Plan shows how you will monitor and maintain cybersecurity
  - Malware free shipping
  - Labeling


Plan for Continuing Support


Plan for Malware Free Shipping

Labeling

Instructions to ensure the safe use of the device

- Interfaces
- Security controls for user interactions
- Network interface instructions
- Logging capabilities and debugging support
- **Manufacturer Disclosure Statement for Medical Device Security (MDS2 or MDS^2)**
- **Software Bill of Materials (if provided to customers)**

Testing To Demonstrate Effective Cybersecurity Controls

Testing Goals

- Demonstrate effectiveness of controls
- Scope/content - covers appropriate functionality
- How identified issues are addressed
- Leverage existing standards/guidance, recognizing limitations

UL 2900 series
IEC 80001 series
ANSI/ISA 62443-4 series
Joint Security Plan (JSP)

Types of Testing

- Select broad testing methods

- Requirements-based verification
- “Hardening”/removing unnecessary software/functionality
- Network Testing
- Static and Dynamic Code Analysis
- Vulnerability Scanning
- Fuzz Testing (Malformed input)
- Penetration testing

Types of Testing

- Select broad testing methods

- Comprehensive and detailed penetration testing can be good indicator of the device security

- Requirements-based verification
- "Hardening"/removing unnecessary software/functionality
- Network Testing
- Static and Dynamic Code Analysis
- Vulnerability Scanning
- Fuzz Testing (Malformed input)
- **Penetration testing**

Third Party Testing

- Information to include:
  - Original third party report
  - Scope of third party engagement
  - Manufacturer's report assessing findings
    - how you addressed
- May also include OTSS vulnerability assessment
- Date of assessment should reflect rapid evolution of cybersecurity risks (reconsider beyond 6 months)

Common Issues Impacting a Successful Premarket Submission

Common Issues

- Missing test documentation
- Missing secure update process
- Update process that is known to be vulnerable
- Cybersecurity controls not linked to risks

Common Issues

- Many issues associated with OTS Software
  - Out of date OTS versions
  - Unsupported OS versions (e.g., Windows XP/7)
  - Not considering security risks associated with OTS
- Unused ports not disabled
- Configurable Security Controls not ON

Common Issues

- Using Bluetooth for safety critical functions
- Use cyclic redundancy checks (CRC) as security controls
- Don’t disclose residual risks to inform user’s own risk management
  - this is shared responsibility
- Involving cybersecurity expertise too late

Knowledge Check

Which is not part of a cybersecurity review?

1. Risk Management
2. Labeling
3. Social media survey
4. Interoperability

Knowledge Check

Cybersecurity risks are unrelated to safety-related risks

1. True
2. False
3. It depends

Summary

- Cybersecurity is a critical aspect in all phases of device's lifecycle
- Cybersecurity documentation is end-to-end
- Effective testing is challenging but vital

Resources

Slide Number	Cited Resource	URL
9	Cybersecurity Postmarket Guidance	www.fda.gov/media/95862/download
9	Cybersecurity Premarket Guidance (2014)	www.fda.gov/media/86174/download
12	Cybersecurity Premarket Guidance draft (2018)	www.fda.gov/media/119933/download
17	CVSS Common Vulnerability Scoring System	www.first.org/cvss/specification-document
19	OTS Networked Cybersecurity Guidance	www.fda.gov/media/72154/download
19	OTS Software in Medical Devices	www.fda.gov/media/71794/download
21	Interoperable Medical Devices	www.fda.gov/media/95636/download

Questions


FDA
U.S. FOOD & DRUG
ADMINISTRATION