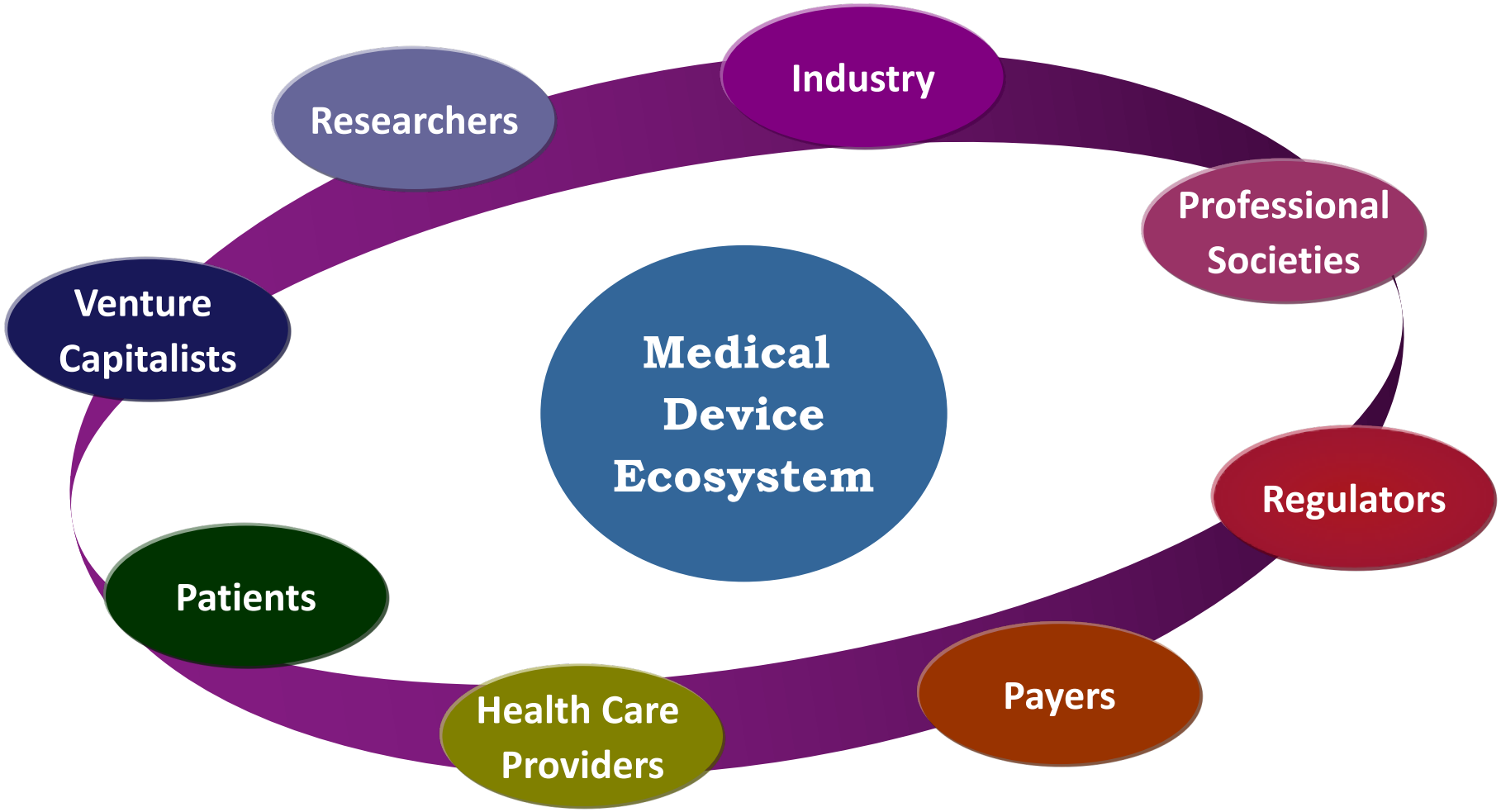
MEDICAL DEVICE CYBERSECURITY: WORKING TOWARD MORE SECURE HEALTHCARE

SETH D CARMODY, PHD, HCISPP
CDRH / FDA

MAY 1, 2019

A Complex Ecosystem



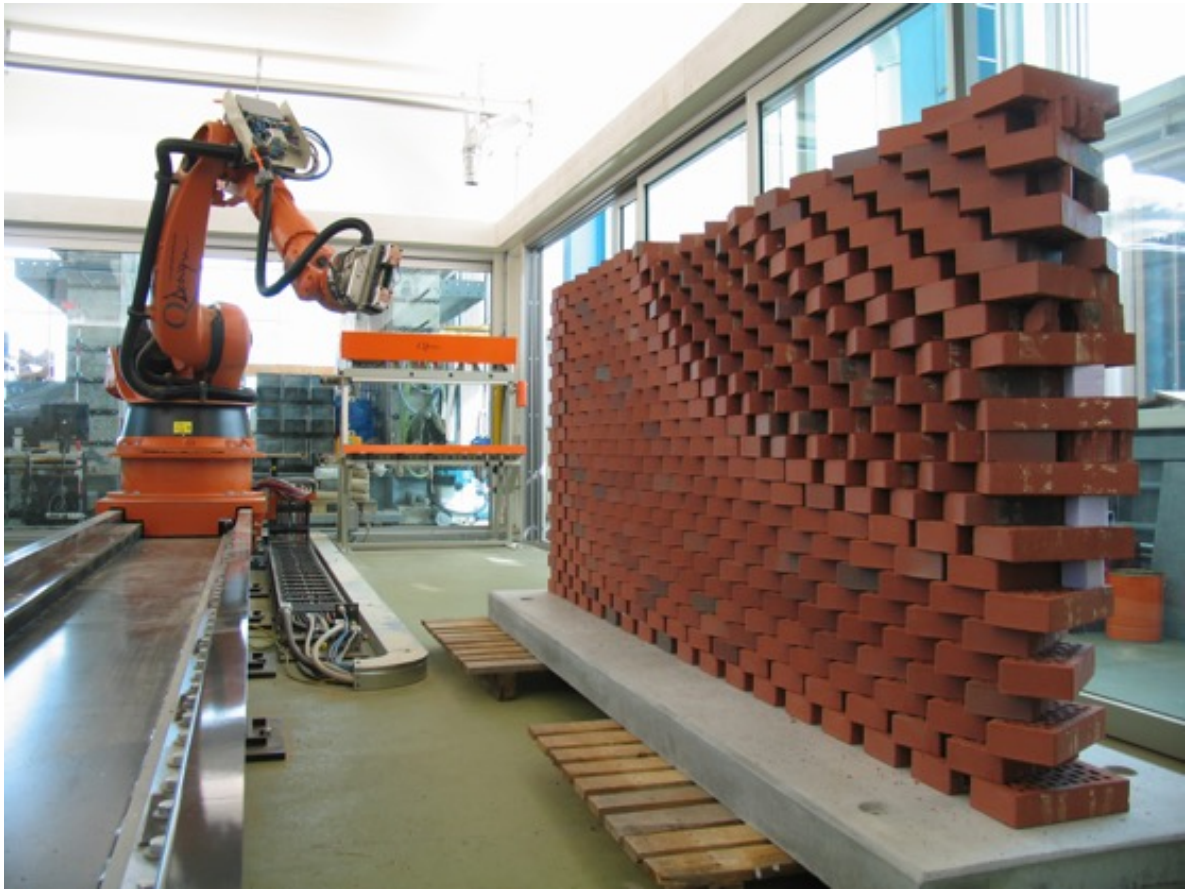
Bricks are Safe

Until Thrown…

https://www.lowes.com/pl/Brick-fire-brick-Asphalt-concrete-masonry-Building-supplies/4294515411

Intended Use + Misuse

http://hackaday.com/2015/09/07/brick-laying-robot-does-it-better/



http://www.technologyvista.in/pin/here-comes-the-brick-laying-robot-to-make-buildings/

What is Security?

"… software engineering is about *ensuring that certain things happen* …, **security is about ensuring that they don't**"[2]

[2] Ross Anderson. *Security Engineering*. 2nd Ed. Wiley, 2008. pp. 4.

Infinite Negative Requirements!

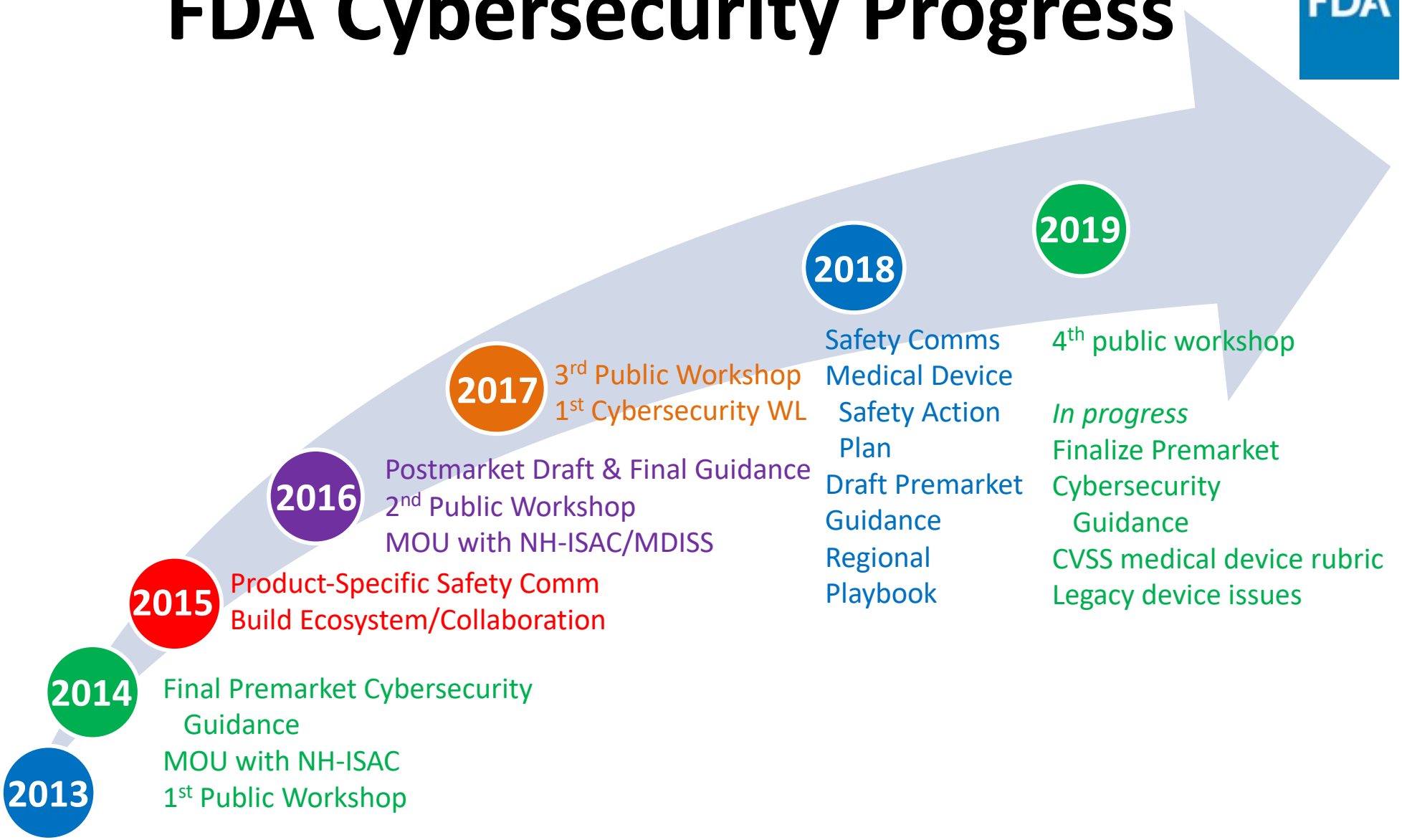
Features:
What a Device MUST Do…
Get drug libraries from the Internet

Thou, shall not under or over deliver therapy!

Safety:
What a Device MUST NOT do

Hackerman – Movie, Kung Fury 2015

FDA Cybersecurity Progress



Medical Device Safety Action Plan:
Advancing Medical Device Cybersecurity

- Update 2014 premarket guidance
- Consider seeking additional premarket and postmarket authorities to:
  - Require that firms build capabilities to update and patch device security into a product's design and to include appropriate data supporting this capability in premarket submissions to FDA for review
  - Require firms to develop a "Software Bill of Materials" (SBOM) and to share with customers
  - Require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified
- Request appropriations for seeding establishment of a CyberMed Safety (Expert) Analysis Board (CYMSAB) functioning as a public-private model, and serving the ecosystem as a neutral entity

Lessons Learned—Evolving Our Thinking

- Coordinated vs. non-coordinated disclosure of device vulnerabilities
  - Ability to get to ground truth as fast as possible so that mitigations can be proactively communicated and executed in a timely manner
    - JnJ Animas Insulin Pump
  - Non-coordinated disclosure results in delayed assessments, communications, and mitigations
    - St Jude/Abbott pacemakers and ICDs
- Impact on HPH critical infrastructure and potential disruption of clinical care
  - Patching operating system is not routine with safety-critical systems
    - WannaCry Global Cyber Attack (May 2017)
    - Petya/notPetya (July 2017)
  - Delays in diagnosis/treatment intervention can result in patient harm too
- Potential for multi-patient (i.e., scaled) attack of highest concern for harm

2018 Premarket Draft Guidance: Revision Background

- New guidance is needed as medical device cybersecurity continues to evolve
- Changes proposed to the guidance based on lessons learned from routine vulnerability management, response activities, engaging stakeholders including working with manufacturers pre- and post-market.
- Examples of recent threats:
  - Malware/ransomware attacks, e.g., WannaCry, notPetya, Meltdown and Spectre

Revision Approach

- Leveraged the 2014 premarket guidance document
  - Kept alignment with NIST 5 core functions
  - Similar structure
  - Maintained focus on documentation related to requirements of the QSR (21 CFR Part 820)

- Provided additional granularity to help manufacturers implement cybersecurity in the premarket setting
  - Expanded on maintaining properties of authenticity, availability, integrity, and confidentiality through design, risk management, and labeling
  - Labeling grounded in statutory and regulatory requirements; for example:
    - Adequate directions for use, 21 CFR 801.5
    - For prescription devices, 21 CFR 801.109(c)

What's New

- Designing trustworthy devices
- Preventing multi-patient attacks
- Tiering system – information to be provided in premarket submission is geared to level of risk:
  - Tier 1 – higher risk
  - Tier 2 – lower risk
- Cybersecurity Bill of Materials
  - Leverages purchasing controls in QSR (21 CFR 820.50)
- System level threat models

Tier Criteria

Tier 1 "Higher Risk"

A device is a Tier 1 device if the following criteria are met:

- The device is capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, or to a network, or to the Internet; AND

- A cybersecurity incident affecting the device could directly result in patient harm to multiple patients.

Examples of Tier 1 devices, include but are not limited to, implantable cardioverter defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps, and the supporting connected systems that interact with these devices such as home monitors and those with command and control functionality such as programmers.

Tier 2 "Standard Risk"

- A medical device for which the criteria for a Tier 1 device are not met.

Tiers Drive Submission Content

- For Tier 1 devices documentation should demonstrate how the device design and risk assessment incorporate the cybersecurity design controls described in the guidance.
- For Tier 2 devices documentation should demonstrate through risk-based rationales why certain cybersecurity design controls are not necessary

- Submitted documentation may include the demonstration of comparable and/or additional cybersecurity design controls that may not be described in the guidance.
- We recommend industry utilize the FDA presubmission process to discuss design considerations for meeting adequacy of cybersecurity risk management throughout the device life-cycle.

Postmarket Cybersecurity Risk Assessment

Assessing Exploitability with Common Vulnerability Scoring System (CVSS)

- **Establish a repeatable process by leveraging existing frameworks (e.g. CVSS)**

Base Scoring (risk factors of the vulnerability)
e.g. Attack Vector (physical, local, adjacent, network)

Temporal Scoring (risk factors that change over time)
e.g. Exploit Code Maturity (high, functional, proof-of-concept, unproven)

Environmental scoring (controls that reduce risk)
e.g. Physical, software, network, compensating controls.

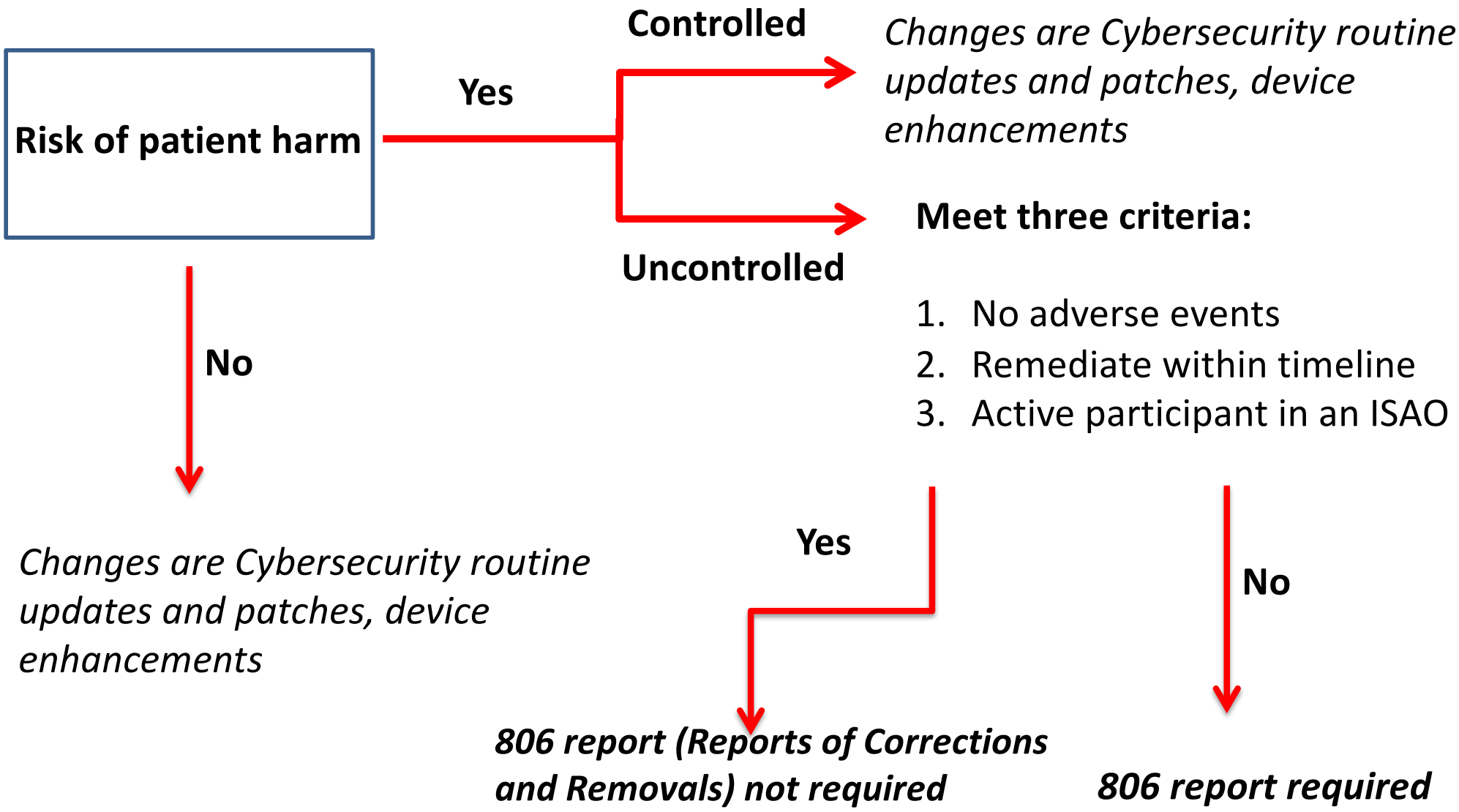
CVSS – Common Vulnerability Scoring System https://www.first.org/cvss

Assessing Severity

Common Term	Possible Description
Negligible	Inconvenience or temporary discomfort
Minor	Results in temporary injury or impairment not requiring professional medical intervention
Serious	Results in injury or impairment requiring professional medical intervention
Critical	Results in permanent impairment or life-threatening injury
Catastrophic	Results in patient death

ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – 441Application of Risk Management to Medical Devices:

Changes to a Device for Controlled vs. Uncontrolled Risk



Distinguishing Medical Device Recalls from Medical Device Enhancements

ISAO (Information Sharing and Analysis Organization)

2018 - 2019 Reflections

- Medical Device Safety Action Plan (April 2018)
- AAMI BI&T: The Evolving State of Medical Device Cybersecurity March/April 2018
- Perspective piece in American Heart Association Journal 'Circulation' (Sept 2018)
- Report on Advancing Coordinated Vulnerability Disclosure – MDIC publication (Oct 2018)
- FDA Commissioner's Statement (Oct 2018):
  - Strong commitment to efforts that bolster medical device cybersecurity
  - Regional Incident Preparedness & Response Playbook – MITRE publication (Oct 2018)
  - Execution of 3-way MOUs with H-ISAC for 2 newly stood up ISAOs for medical device vulnerability reporting (Oct 2018):
    - MedISAO
    - Sensato

2018 -2019 Reflections continued

- New FDA Draft Premarket Cybersecurity Guidance
- Execution of MOA with Department of Homeland Security
- HSCC Task Group 1B released Joint Security Plan Jan 28, 2019
- FDA convened Public Workshop, Jan 29-30, 2019

Looking Ahead 2019

- Complete CVSS clinical rubric & submit for MDDT qualification (MITRE-led WG)
- Further enhance public-private partnership collaborations to collectively address Imperative 2 of 2017 Task Force Report:
  - CYMSAB Pilot currently under development (with MITRE support)
  - Additional ISAOs in formation for device vulnerability info-sharing
  - Dedicated effort on defining and operationalizing Software Bill of Materials

Looking Ahead 2019 continued

- International Medical Device Regulators Forum (IMDRF) new medical device cybersecurity work item:
  - FDA and Health Canada co-leads
- Expand x-stakeholder participation in DefCon Biohacking Village Device Hacking Lab, with the following goals:
  - Increase medical device manufacturer (MDM) presence
  - Introduce to clinical community
  - Engage HDOs
- Leverage cross-agency / multi-stakeholder collaborative efforts:
  - NTIA (Dept of Commerce) Multi-stakeholder engagement on software component transparency includes representation on WGs from: HDOs, MDMs, device trade organizations and FDA
  - NCCoE (NIST/Dept of Commerce) working with industry to develop use cases for medical device security

Medical device cybersecurity is a shared responsibility

FDA contacts:

Suzanne.Schwartz@fda.hhs.gov
Seth.Carmody@fda.hhs.gov
Aftin.Ross@fda.hhs.gov

Or email the team:

CyberMed@fda.hhs.gov

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm