MEDICAL DEVICE CYBERSECURITY

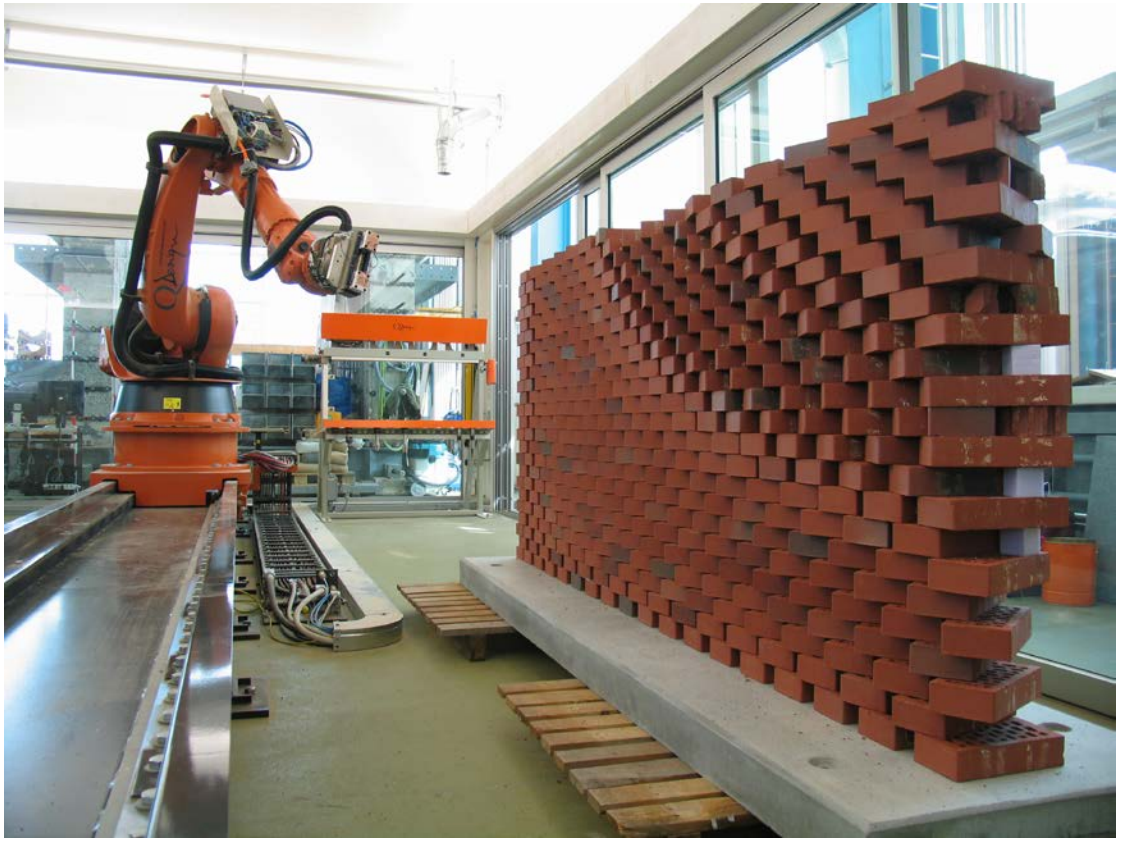
SETH D. CARMODY, PHD

APRIL 30, 2018

SMART WORKSHOP

Intended Use + Malicious 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/

Negative Requirements are *Infinite*!

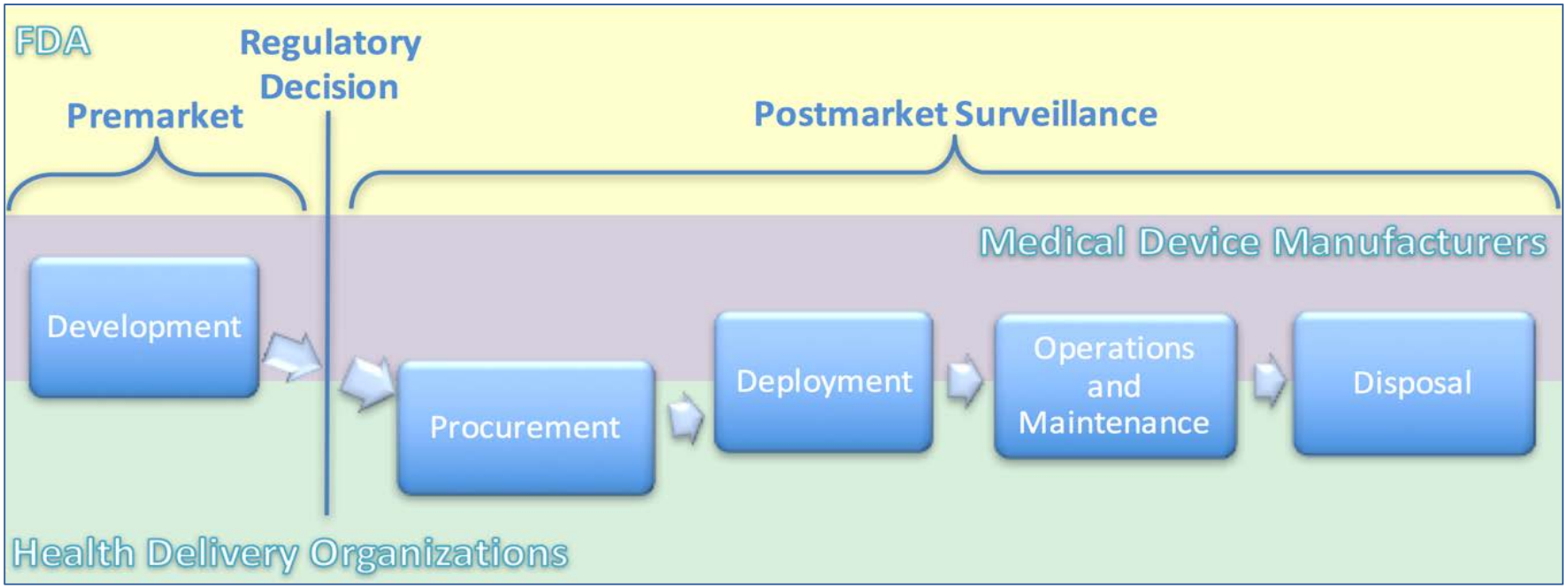
Features:
What a Device MUST Do…
Get drug libraries from the Internet

Thou, shall not under or over deliver therapy!

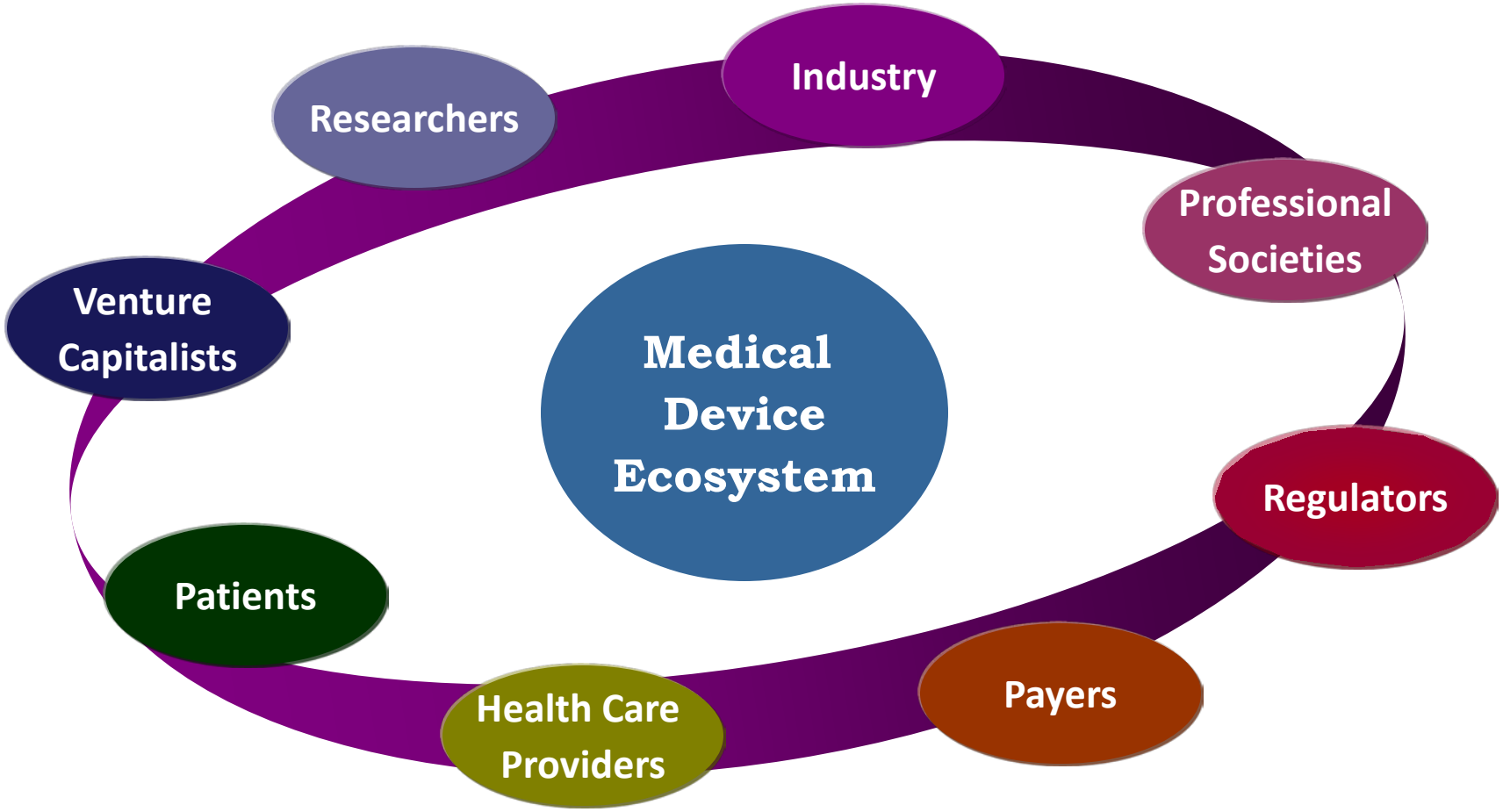
Safety:
What a Device MUST NOT do

Hackerman – Kung Fury, 2015

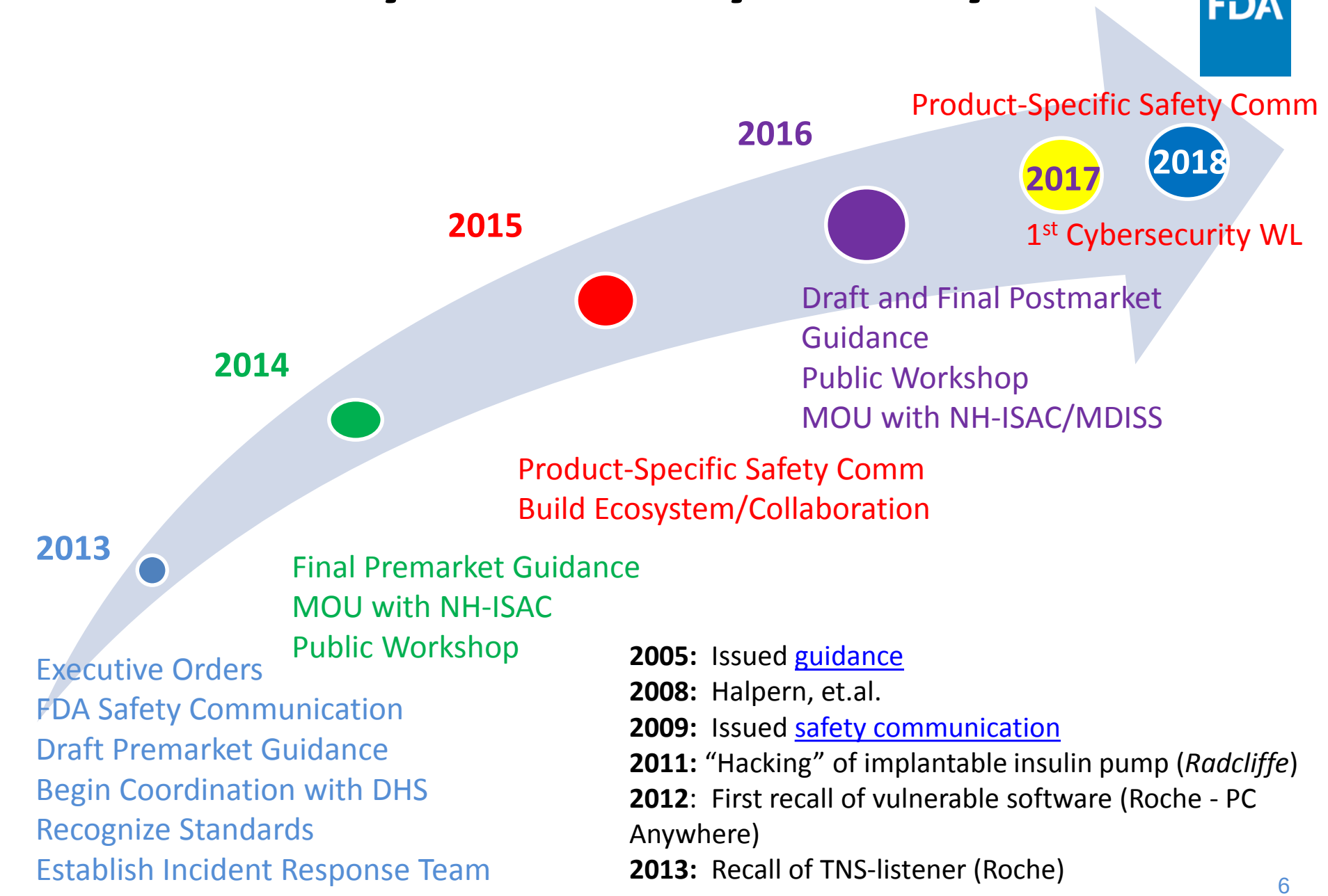
Device Lifecycle: Ecosystem Challenges



Diverse Stakeholders



FDA Cybersecurity History



2005: Issued guidance
2008: Halpern, et.al.
2009: Issued safety communication
2011: "Hacking" of implantable insulin pump (*Radcliffe*)
2012: First recall of vulnerable software (Roche - PC Anywhere)
2013: Recall of TNS-listener (Roche)

Premarket Cybersecurity Guidance

- Draft June 2013
- Final October 2014
- Key Principles:
  - #1 Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
  - #2 Address cybersecurity during the design and development of the medical device
  - #3 Establish design inputs for device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g)

Key Principles of FDA Postmarket Management of Cybersecurity in Medical Devices

- Use a risk-based framework to assure risks to public health are addressed in a continual and timely fashion
- Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and postmarket authorities
- Foster a collaborative and coordinated approach to information sharing and risk assessment
- Align with Presidential EOs and NIST Framework
- Incentivize the “right” behavior

Postmarket Cybersecurity Risk Assessment

Assessing Exploitability with Common Vulnerability Scoring System (CVSS)

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

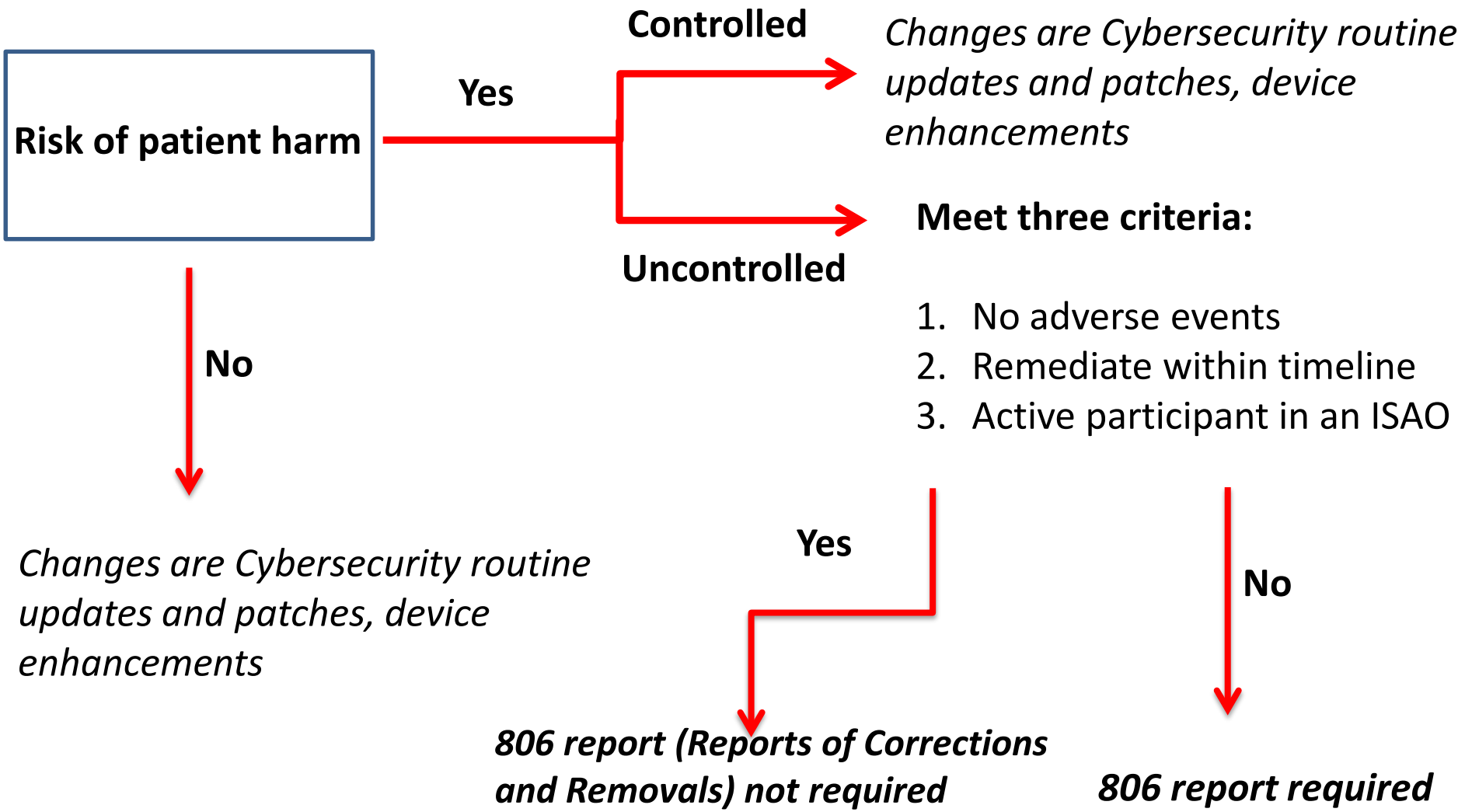
Base Scoring (risk factors of the vulnerability)
e.g. Attack Vector (physical, local, adjacent, network)

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

Changes to a Device for Controlled vs. Uncontrolled Risk



Distinguishing Medical Device Recalls from Medical Device Enhancements

ISAO (Information Sharing and Analysis Organization)

Controlled Vulnerabilities

"Acceptable Residual Risk"

- Promote good cyber hygiene and reduce cybersecurity risks even when residual risk is acceptable
- Changes to a device solely to strengthen the cybersecurity associated with vulnerability with controlled risk are referred to as cybersecurity routine updates and patches and are typically considered to be device enhancements and are not required to be reported
- Annual reporting requirements for premarket approval (PMA) devices

Uncontrolled Vulnerabilities

"Unacceptable Residual Risk"

- Reporting Requirements:
  - Manufacturers (MDM) are required to report uncontrolled vulnerabilities to FDA (21 CFR 806)
  - FDA does not intend to enforce reporting requirements under CFR 806 if all of the following circumstances are met:
    - No known serious adverse events or deaths associated with the vulnerability
    - MDM meets timeline criteria:
      - Within 30 days provides notification to customers, interim control measures, and remediation plan
      - Within 60 days fixes the vulnerability, validates the change, and distributes the deployable fix to its customers and user community.
    - The manufacturer actively participates as a member of an ISAO.
- The manufacturer should evaluate the device changes to assess the need to submit a premarket submission (e.g., PMA, 510(k), etc.) to the FDA
- Remediation of devices with annual reporting requirements (e.g., class III devices) should be included in the PMA annual report, as indicated for controlled vulnerabilities

Questions?

Contacts:

CDRH mailbox, CyberMed@fda.hhs.gov
Dr. Suzanne Schwartz, Suzanne.Schwartz@fda.hhs.gov
Dr. Aftin Ross, Aftin.Ross@fda.hhs.gov
LCDR Cristina Dar, Cristina.Dar@fda.hhs.gov
Dr. Seth Carmody, Seth.Carmody@fda.hhs.gov