Here's What You Must Do

Seth Carmody
Cybersecurity Project Manager,
Emergency Preparedness/Operations & Medical Counter-measures,
CDRH, FDA
Comprehensive Cyber Security Risk Management: Know, Assess, Fix

Seth D. Carmody, Ph.D.
Center for Devices and Radiological Health, FDA
Medical Design Group, October Forum
October 5, 2016
Main Points

• No legislative risk panacea
• Benefit – Risk is Key
• Establish a Cybersecurity Risk Management Program
  – Know, Assess, and Address risks:
    • Resources and best practices are prevalent
      – Research and development
    • Risks continually evolve
      – When devices are deployed
      – Software updates for cybersecurity do not typically require pre-market review or recall
      – Define Responsibilities with Customers
Healthcare Sector Challenges

1. Lack of Cybersecurity Culture
2. Unpredictable threats
3. Difficult risk quantification
4. Perceived and real economics
5. Procurement
6. Multiple and diverse stakeholders
7. Technical requirements
4 Forces of Maturity

1. FDA
2. Procurement
3. Reimbursement
4. Liability

http://software.gsfc.nasa.gov/docs/What%20is%20CMMI.ppt
Draft Guidance: Postmarket Management of Cybersecurity in Medical Devices – *Key Principles*

- Align with Presidential EOs and NIST Framework
- Risk-based framework to assuring risks to public health are addressed in a timely fashion
- Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and postmarket authorities
- Collaborative approach to information sharing and risk assessment
- Incentivize the “right” behavior
Essential clinical performance (ECP) means performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer.

Compromise of the essential clinical performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm.

• A new concept, derived from IEC 60601
Assessment Challenges

- Calculating exploitability is difficult due to the active adversary.
  - Does $P_1 = 1$? (assume exploit?)
  - All systems fail?
  - “There are as many motivations for hacking as there are people” – Josh Corman, I Am the Cavalry

- Not all vulnerabilities will have an uncontrolled impact to the essential clinical performance. This is the main differentiation between medical safety and IT security worlds.

- Complications due to vulnerability chaining. Threats may leverage multiple, possibly low risk vulns. chained together to amplify risk

- What devices are impacted?
  - Vertical and horizontal analysis
  - Bill of materials
What Happens if I Fix?

Depends on why you are fixing

1. Improving quality?
2. Is there risk to health?
3. Is there a violation?

See 21 CFR § 806.1(b)(1)
Different Risk: Two Types of Fixes

Risk to essential clinical performance

Yes

Uncontrolled

Controlled

Device enhancement (fix)

Three criteria:

1. No adverse events
2. Mitigate (fix) in 30 days
3. Participate in an ISAO

Yes

No reporting under 806

Distinguishing Medical Device Recalls from Medical Device Enhancements

ISAO (Information Sharing and Analysis Organization)
The ISAO best practice models are intended to be:

**Inclusive** - groups from any and all sectors, both non-profit and for-profit, expert or novice, should be able to participate in an ISAO;

**Actionable** - groups will receive useful and practical cybersecurity risk, threat indicator, and incident information via automated, real-time mechanisms if they choose to participate in an ISAO;

**Transparent** - groups interested in an ISAO model will have adequate understanding of how that model operates and if it meets their needs; and

**Trusted** - participants in an ISAO can request that their information be treated as Protected Critical Infrastructure Information. Such information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt from regulatory use and civil litigation.

See: [http://www.dhs.gov/isao](http://www.dhs.gov/isao)
Next Steps

- Development and validation of meaningful tools for assessment of vulnerabilities in the clinical environment is an area of focus going forward
- Definition of the medical device Information Sharing and Analysis Organization model
- Outreach, outreach, outreach
- Consolidated resource page
- Internal and external training
  - How are we ensuring that our policies are effective?
- Contact: Seth.Carmody@fda.hhs.gov

Thank You & Questions?