MEDICAL DEVICE CYBERSECURITY: FDA APPROACH

CYBERMED SUMMIT
JUNE 9TH, 2017

SUZANNE B. SCHWARTZ, MD, MBA
ASSOCIATE DIRECTOR FOR SCIENCE & STRATEGIC PARTNERSHIPS
CENTER FOR DEVICES AND RADIOLOGICAL HEALTH
US FOOD & DRUG ADMINISTRATION

"Safeguarding our Patients: Harnessing the Collective Will & Creating a Culture of Multi-Stakeholder Collaboration for Medical Device Security"

Bottom Line Up Front

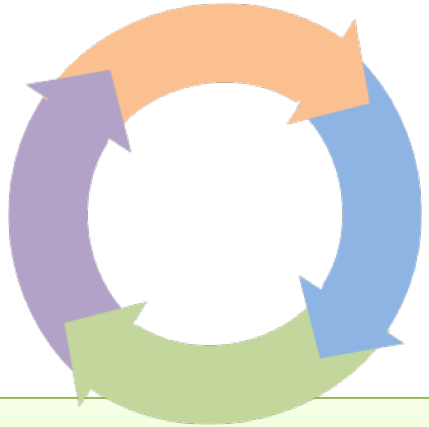
- Foster culture of *continuous quality improvement* and underpinning of total product life cycle (TPLC) approach
- Implement a proactive, comprehensive risk management program
  - Apply the National Institute of Standards and Technology (NIST) Framework to Strengthen Critical Infrastructure Cybersecurity
  - Establish and communicate processes for vulnerability intake and handling
  - Adopt a coordinated disclosure policy and practice
  - Deploy mitigations that address cybersecurity risk early and prior to exploitation
- Engage in collaborative information sharing for cyber vulnerabilities and threats

Envisioning a Positive Feedback Loop across the Ecosystem

Post market surveillance

Regulatory clarity

- *Premarket expectations*
- *Post market expectations*



Stake holder collaboration

- *Device industry*
- *Healthcare providers*
- *Federal partners*
- *Researchers & experts*

Enable a platform for maintaining Cybersecurity Awareness –

Intentional and unintentional threats

Key Medical Device Cybersecurity Myth Busters

- **Myth:** Manufacturers are not permitted to make updates to devices for cybersecurity without going back to FDA first for "re-certification"
- **Fact:** Most medical device software changes made solely to strengthen cybersecurity do not require pre-market review or product recall (there are some exceptions).

- **Myth:** Cybersecurity of medical devices is voluntary for medical device manufacturers and not enforceable.

- **Fact:** Medical device manufacturers are required by law to comply with all applicable regulations, including the quality system regulations (QSRs). The pre- and post-market cybersecurity guidances articulate that a comprehensive, structured and systematic cybersecurity risk management program is necessary under the Quality System Regulation.

Framing The Issue: Environment

- The health care and public health (HPH) critical infrastructure sector represents a significantly large attack surface for national security today
  - Intrusions and breaches occur through weaknesses in the system architecture
- Connected medical devices, like all other computer systems, incorporate software that are vulnerable to threats
- We are aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations
- When medical device vulnerabilities are not addressed and remediated, they can serve as access points for entry into hospital/health care facility networks
  - May lead to compromise of data confidentiality, integrity, and availability

Executive Orders (EO), Presidential Policy Directives (PPD), and NIST Framework to Strengthen Critical Infrastructure Cybersecurity

- EO 13636 (Feb 2013)

"We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

- PPD 21 (Feb 2013)
- NIST Framework to Strengthen Critical Infrastructure Cybersecurity (Feb 2014)
- EO 13691 (Feb 2015) – establishment of Information Sharing and Analysis Organizations (ISAO)

Systemic Challenges – 2014 FDA Workshop Findings

- Growing cyber threat
- Cybersecurity may not be on the radar of the C-suite
- No safe space for information-sharing
- Lack of a common lexicon
- Lack of standards for device integration and maintenance
- No one-size fits all solution
- *Cybersecurity isn't just a design issue; it's a lifecycle issue*
- Incomplete rules of engagement

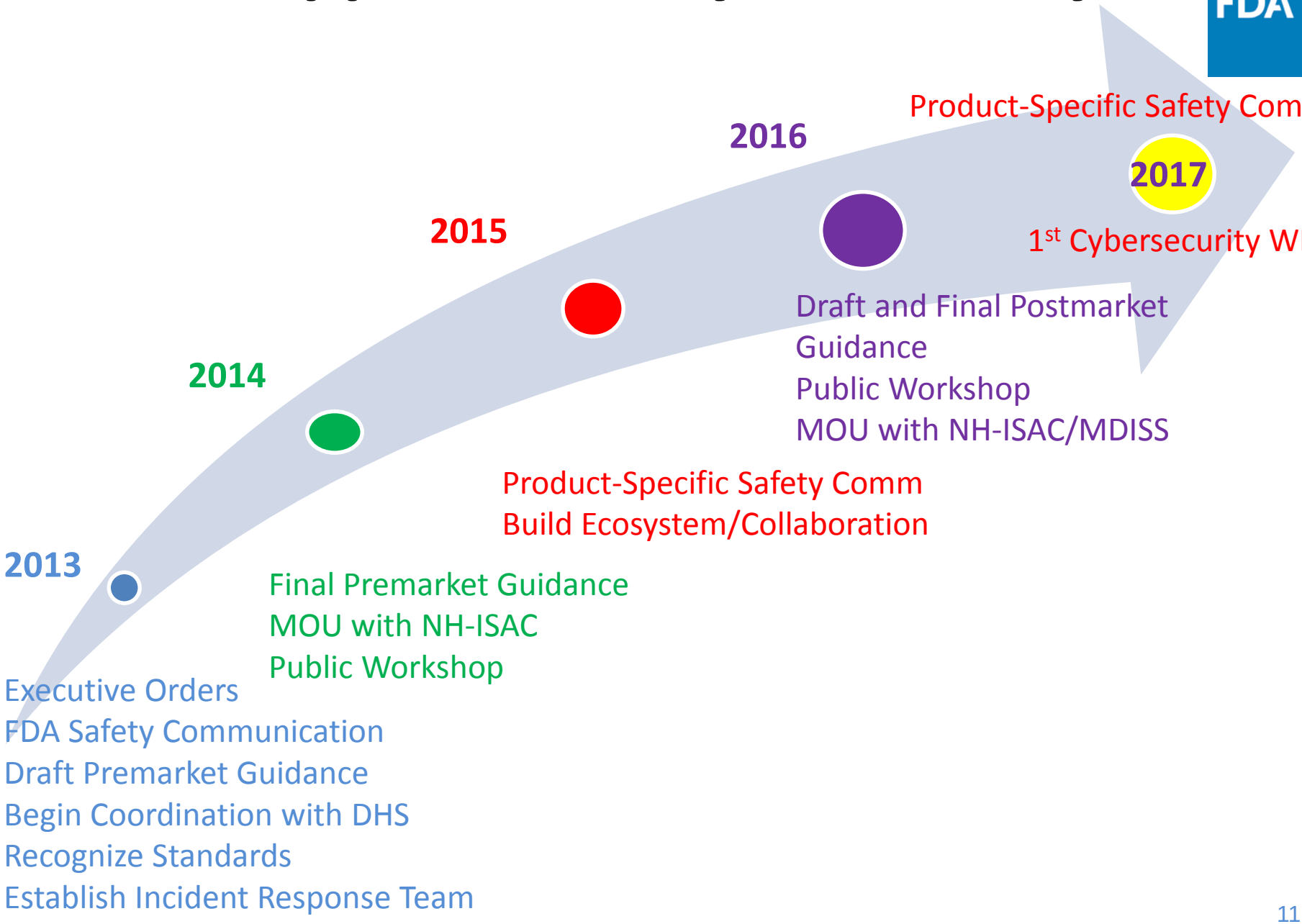
Stakeholder Challenges - 2014 FDA Workshop Findings

- Lack of trust
- Many stakeholders addressing cybersecurity in silos
    - Some may not understand the clinical environment
- Cyber-researchers bring disruption to the community
- A lot of smaller organizations without the cybersecurity resources or expertise

Stakeholder Challenges -2014 FDA Workshop Findings continued

- Stakeholders don't know how to prioritize vulnerabilities
- Stakeholders may not know all of the standards and tools that exist and which are best
- *What is the value proposition?*

FDA's Approach to Cybersecurity



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

What's Changed From Draft to Final Postmarket Guidance

- 30 day remediation timeframe has been expanded to include a 60 day tier
- In alignment with current FDA-recognized standards, essential clinical performance is now safety and essential performance scoped to patient harm
- With respect to ISAOs, we clarified the definition of active participation by providing specific criteria
- The scope has been clarified with respect to privacy and confidentiality harms

Cybersecurity – Assessing Risk

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

- Severity of Patient Harm (if the vulnerability were to be exploited)
- Exploitability

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)
Attack Vector (physical, local, adjacent, network)
Attack Complexity (high, low)
Privileges Required (none, low, high)
User Interaction (none, required)
Scope (changed, unchanged)

Confidentiality Impact (high, low, none)
Integrity Impact (none, low, high)
Availability Impact (high, low, none)

Temporal Scoring (risk factors that change over time)
Exploit Code Maturity (high, functional, proof-of-concept, unproven)
Remediation Level (unavailable, work-around, temporary fix, official fix, not defined)
Report Confidence (confirmed, reasonable, unknown, not defined)

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:

Information Sharing and Analysis Organizations (ISAO) – What are they?

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.

An example of an ISAO is the National Health Information Sharing & Analysis Center (NH-ISAC)

DHS: http://www.dhs.gov/isao

NH-ISAC: https://nhisac.org/announcements/nh-isac-and-mdiss-partner-to-form-medical-device-security-information-sharing-initiative/

Criteria for Defining Active Participation by a Manufacturer in an ISAO

Active participation by a manufacturer in an ISAO can assist the company, the medical device community and the HPH Sector by proactively addressing cybersecurity vulnerabilities and minimizing exploits through the timely deployment of risk control measures including communication and coordination with patients and users.

FDA will consider a manufacturer to be an active participant in an ISAO if:

- The manufacturer is a member of an ISAO that shares vulnerabilities and threats that impact medical devices;
- The ISAO has documented policies pertaining to participant agreements, business processes, operating procedures, and privacy protections;
- The manufacturer shares vulnerability information with the ISAO, including any customer communications pertaining to cybersecurity vulnerabilities;
- The manufacturer has documented processes for assessing and responding to vulnerability information, threat intelligence, medical device risk assessments, countermeasure solutions, cyber incident response approaches, and best practices received from the ISAO that impacts their medical device product portfolio.

Changes to a Device for Controlled vs. Uncontrolled Risk

Risk of patient harm

Yes

Controlled

Changes are Cybersecurity routine updates and patches, device enhancements

Uncontrolled

Meet three criteria:

1. No adverse events
2. Remediate within timeline
3. Active participant in an ISAO

No

Changes are Cybersecurity routine updates and patches, device enhancements

Yes

Part 806 report (Reports of Corrections and Removals) not required

No

Part 806 report required

[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"

Guidance Addresses:

- Reporting Requirements
- Time Frame for Mitigating Risks
- Public Disclosure
- Information Sharing and Stakeholder Collaboration

Uncontrolled Vulnerabilities Approach

- Manufacturers are expected to report these vulnerabilities to the FDA according to 21 CFR 806 (Reports of Corrections and Removals)
- 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**
    - **Remediate within a tiered 30 and 60 day timeline**
    - **The manufacturer actively participates as a member of an ISAO that shares vulnerabilities and threats that impact medical devices, such as NH-ISAC (see section IX) and provides the ISAO with any customer communications upon notification of its customers.**
- 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

Key Takeaways

- Foster culture of *continuous quality improvement* and underpinning of total product life cycle (TPLC) approach
- Implement a proactive, comprehensive risk management program
  - Apply the National Institute of Standards and Technology (NIST) Framework to Strengthen Critical Infrastructure Cybersecurity
  - Establish and communicate processes for vulnerability intake and handling
  - Adopt a coordinated disclosure policy and practice
  - Deploy mitigations that address cybersecurity risk early and prior to exploitation
- Engage in collaborative information sharing for cyber vulnerabilities and threats

Thank You!

For Specific Questions Related to the Postmarket Cybersecurity Final Guidance: AskMedCyberWorkshop@fda.hhs.gov

FDA Medical Device Cybersecurity Informational Webpage: https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

For General Questions about FDA and Medical Device Cybersecurity:
Suzanne.Schwartz@fda.hhs.gov
Seth.Carmody@fda.hhs.gov