Speaker Introduction

Suzanne B. Schwartz, M.D., MBA
Associate Director for Science and Strategic Partnerships
Center for Devices and Radiological Health
U.S. Food and Drug Administration
Conflict of Interest

Suzanne B. Schwartz, M.D., MBA

Has no real or apparent conflicts of interest to report.
Agenda

• Background
• Total Product Life Cycle (TPLC) Framework
• Premarket & Postmarket Cybersecurity Approach
• What’s Changed
• Key Terms
• Cybersecurity Risk Assessment
• Information Sharing and Analysis Organization (ISAO)
• Controlled and Uncontrolled Vulnerabilities
• Key Messages
Learning Objectives

• Identify the roles of the FDA and Joint Commission for driving adoption of security best practices and health risk reduction through regulatory and accreditation based actions

• Describe how health systems will be impacted by emerging regulation and accreditation policy and actions

• Discuss the challenges and opportunities from the front lines of healthcare delivery
An Introduction of How Benefits Were Realized for the Value of Health IT

- Medical technology companies create life changing innovation -- allowing people to live longer, healthier and more productive lives.
- Medical technology advancements yield savings across the health care system by replacing more expensive procedures, reducing hospital stays and allowing people to return to work more quickly.
- The advanced medical technology industry is fueled by small businesses and entrepreneurs, providing high quality jobs and economic growth in communities both large and small.
- In order to advance the benefits of medical technology and ensure continued American leadership of this industry, we must have the right public policies to support investment, innovation and patient access.

http://www.advamed.org/issues/value-medical-technology
Bottom Line Up Front

- 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
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)
FDA’s Approach to Cybersecurity

- **2013**: Executive Orders, FDA Safety Communication, Draft Premarket Guidance, Begin Coordination with DHS, Recognize Standards, Establish Incident Response Team
- **2014**: Final Premarket Guidance, MOU with NH-ISAC, Public Workshop
- **2015**: Product-Specific Safety Comm, Build Ecosystem/Collaboration
- **2016**: Draft & Final Postmarket Guidance, Public Workshop, MOU with NH-ISAC/MDISS
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
Key Terms: Safety and Essential Performance

• Derived from ANSI/AAMI ES60601-1: Medical electrical equipment—Part 1: General requirements for basic safety and essential performance

• Functions of a device which must remain operational in order to fulfill the intended use and that can be disrupted by exploit
Key Term: Patient Harm

- Derived from ANSI/AAMI/ISO 14971: Medical Devices – Application of Risk Management to Medical Devices

- Limited scope to physical harm to patients
  - Changes to devices to address *uncontrolled risk* of patient harm are called *remediations*

- Changes to devices to address *controlled risk* of patient harm and/or other harms would be categorized as *cybersecurity routine updates and patches*
Postmarket Cybersecurity Risk Assessment

Severity of Patient Harm (if exploited)

Negligible  Minor  Serious  Critical  Catastrophic

Exploitability

High
Medium
Low

Uncontrolled Risk

Controlled Risk
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](https://www.first.org/cvss)
<table>
<thead>
<tr>
<th>Common Term</th>
<th>Possible Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>Inconvenience or temporary discomfort</td>
</tr>
<tr>
<td>Minor</td>
<td>Results in temporary injury or impairment not requiring professional medical intervention</td>
</tr>
<tr>
<td>Serious</td>
<td>Results in injury or impairment requiring professional medical intervention</td>
</tr>
<tr>
<td>Critical</td>
<td>Results in permanent impairment or life-threatening injury</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>Results in patient death</td>
</tr>
</tbody>
</table>

ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – Application 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](http://www.dhs.gov/isao)

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
    - 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

- Uncontrolled
  - 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.
Guidance Example: Controlled Risk

- **Vulnerability Identification:** a researcher publicly discloses exploit code for a four year old vulnerability in commercial off-the-shelf database software.
  - The vulnerable version of the software is in a percentage of the manufacturer’s installed base and in two separate product lines including a multi-analyte chemistry analyzer.

- **Vulnerability Assessment and Validation:** The manufacturer determines that the vulnerability is the result of a misconfigured database setting and could allow an unauthorized user to view patient health information in the database.

- **Vulnerability Impact Analysis:** The vulnerability does not permit the unauthorized user the ability to edit/manipulate data in the database.

- **Vulnerability Risk Determination (controlled VS uncontrolled):** Thus, the manufacturer determines the vulnerability has acceptable and **controlled** risk of patient harm.

- **Manufacturer’s Actions include Communication and Appropriate Mitigation:** The manufacturer notifies its customers and the user community of the issue, details the secure configuration setting, and documents the effectiveness of the cybersecurity routine update for the configuration setting.
Guidance Example: Uncontrolled Risk

A vulnerability known to the security community, yet unknown to a medical device manufacturer, is incorporated into a Class II device during development.

- **Vulnerability Identification, Assessment and Validation:** During postmarket, the manufacturer becomes aware of the vulnerability and determines that the device continues to meet its specifications, and that no device malfunctions or patient injuries have been reported. There is no evidence that the identified vulnerability has been exploited.

- **Vulnerability Impact Analysis:** However, it was determined that the vulnerability introduced a new failure mode to the device that impacts its essential performance.

- **Vulnerability Risk Determination (controlled VS uncontrolled):** The manufacturer determines that the device’s design controls do not adequately reduce the risk to an acceptable level. Without additional mitigations, the risk of patient harm is *uncontrolled.*
Guidance Example: Uncontrolled Risk

continued

- **Manufacturer’s Actions including Communications and Appropriate Mitigations:** manufacturer does not have a fix immediately available to mitigate vulnerability impact on the device’s essential performance. Therefore-
  - Within 30 days of learning of the vulnerability the manufacturer notifies its customers, the ISAO, and user community of the cybersecurity risk and instructs them to disconnect the device from the hospital network to prevent unauthorized access to the device. The company’s risk assessment concludes that the risk of patient harm is now controlled with this additional mitigation.
  - Disconnection of the device from the network is only a temporizing measure, not a viable long-term solution. Manufacturer distributes a patch within 60 days of learning of the vulnerability.
  - If the firm is an active participating member of an ISAO, FDA does not intend to enforce compliance with the reporting requirement under 21 CFR part 806.
Key Messages

- Implement a proactive, comprehensive risk management program
  - Apply the 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
A Summary of How Benefits Were Realized for the Value of Health IT

- Patient access to advanced medical technology generates efficiencies and cost savings for the health care system and the economy. Between 1980 and 2010, advanced medical technology helped cut the number of days people spent in hospitals by more than half.†

- Advanced medical devices and diagnostics save lives and improve the quality of patient care. Between 1980 and 2010, medical advancements helped add five years to U.S. life expectancy and reduce fatalities from heart disease and stroke by more than half.†

- The medical device and diagnostics industry is extremely competitive, ensuring that medical technology is a good bargain. Medical device prices in the U.S. increased at an average annual rate of 1.0 percent for the 22 year period from 1989 to 2010 – a rate less than half that of prices in the overall economy and less than one-quarter the rate of prices for other medical goods and services.†

- Medical devices and diagnostics are central to medical practice, but spending on advanced medical technology is consistently a small and stable share of national health expenditures – accounting for about 6 percent of national health expenditures annually from 1992 to 2010.†

Questions

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

For General Questions about FDA and Medical Device Cybersecurity:

- Suzanne.Schwartz@fda.hhs.gov
- Seth.Carmody@fda.hhs.gov

Thank You!