HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

Managing Medical Device Cybersecurity Vulnerabilities

Session 11, March 6, 2018

Seth Carmody, CDRH Cybersecurity Program Manager, FDA Center for Devices and Radiological Health (CDRH)

Penny Chase, IT and Cybersecurity Integrator, MITRE

COMMITMENT

www.himssconference.org

#HIMSS18

MITRE

FDA

Conflict of Interest

Seth Carmody, Ph.D.

Penny Chase, M.S.

Have no real or apparent conflicts of interest to report.

Agenda

- Learning objectives
- FDA's approach to medical device cybersecurity
  - FDA Premarket Cybersecurity Guidance
  - FDA Postmarket Management of Cybersecurity in Medical Devices
- Assessing severity of cybersecurity vulnerabilities in medical devices with Common Vulnerability Scoring System (CVSS)
  - Developing CVSS supplemental rubric
  - Qualifying the rubric as an Medical Device Development Tool (MDDT)
- Summary

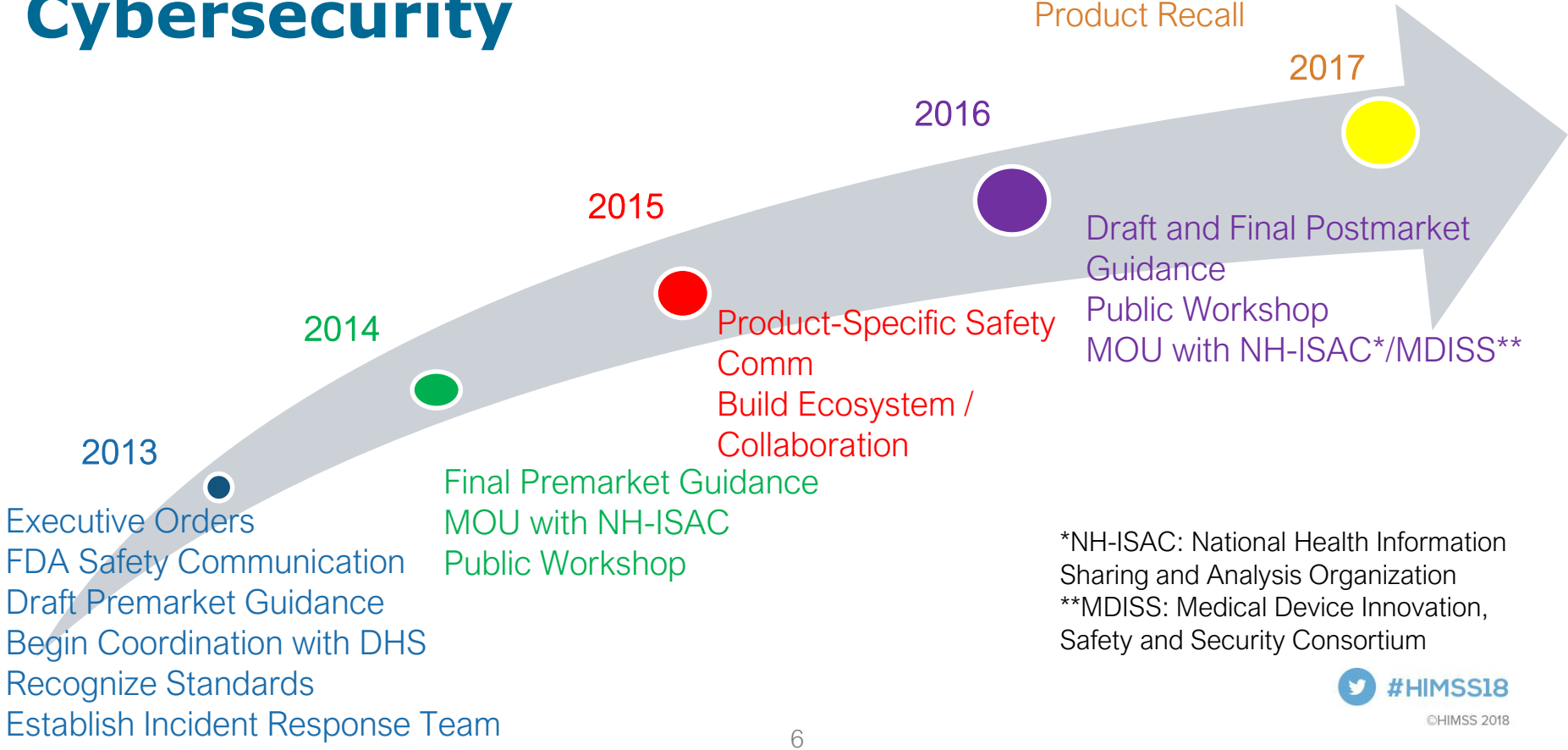
Learning Objectives

- Describe the FDA's Postmarket Management of Cybersecurity in Medical Devices, to include the main policy tenets FDA has put forward that address security throughout the total product lifecycle
- Explain what an Information Sharing and Analysis Organization (ISAO) is and what role they have in helping to facilitate medical device cybersecurity
- Describe the Common Vulnerability Scoring System (CVSS) and how it is being adapted to assess medical device vulnerability impacts
- Discuss the lessons learned from medical device cybersecurity table top exercises and how these insights are being used to improve overall medical device cybersecurity

Framing The Issue: Environment & Impacts to Patient Safety

- 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

FDA's Approach to Cybersecurity



*NH-ISAC: National Health Information Sharing and Analysis Organization
**MDISS: Medical Device Innovation, Safety and Security Consortium

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 Executive Orders and National Institute of Standards and Technology (NIST) Framework
- Incentivize the “right” behavior

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 American National Standards Institute/Association for the Advancement of Medical Instrumentation (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

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

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.

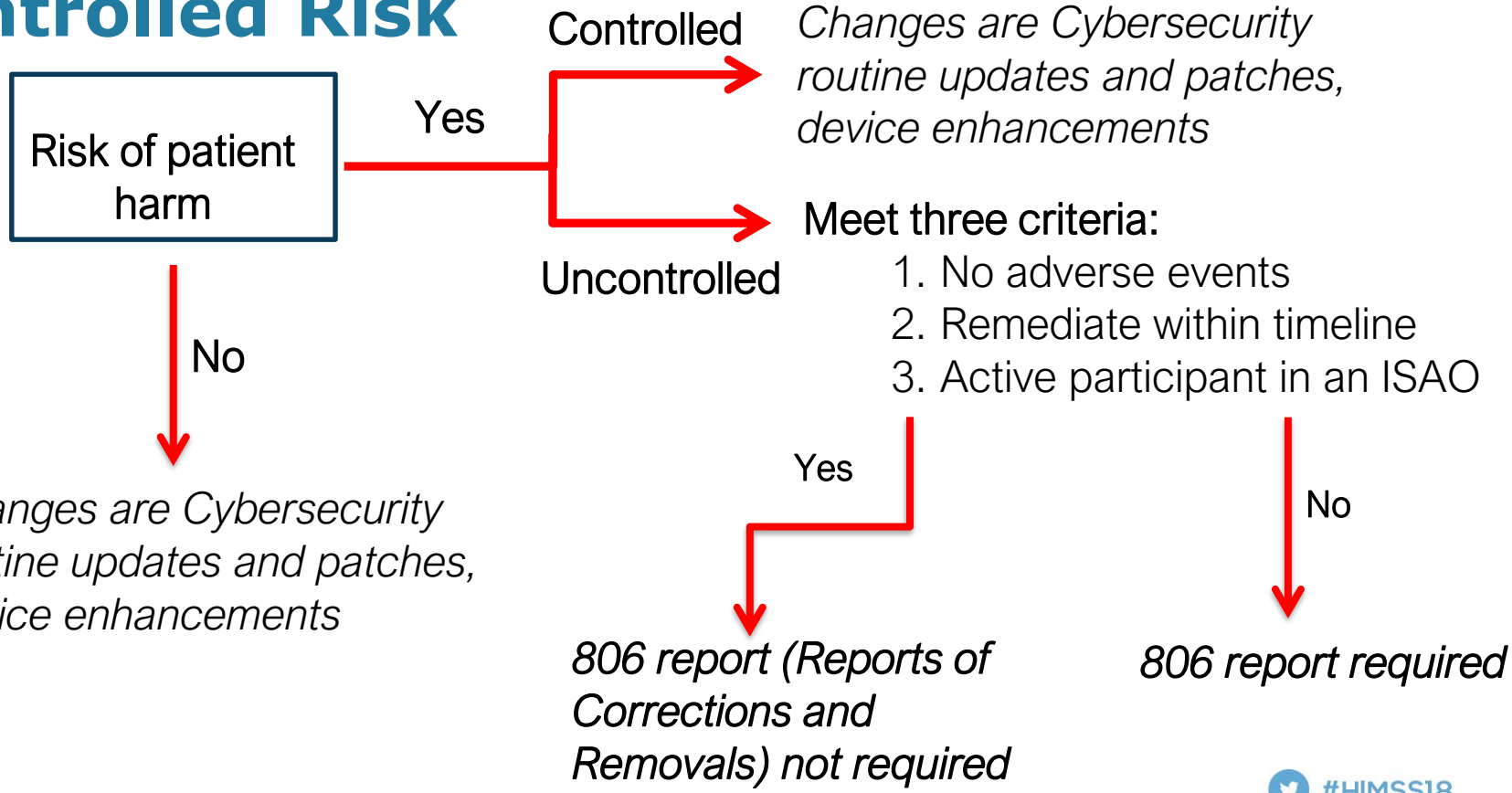
FDA will consider a manufacturer to be an active participant in an ISAO if:

- 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.

Emerging ISAOs

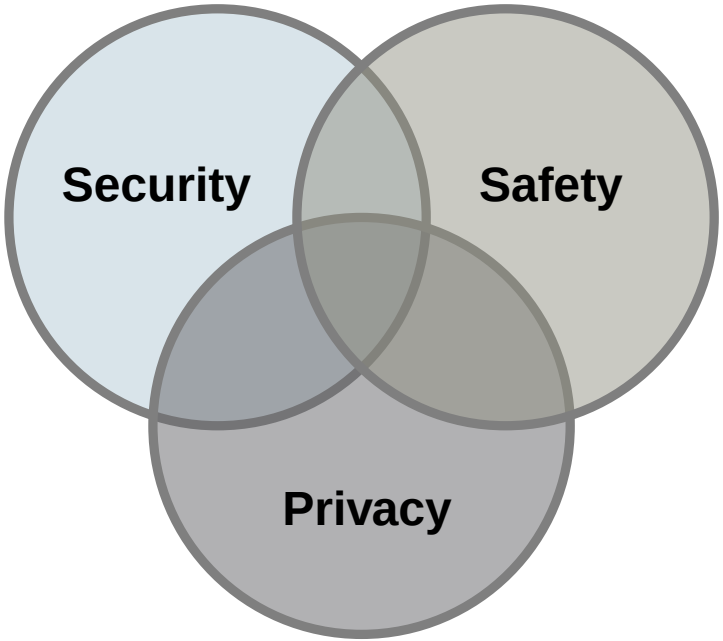
- As FDA has encouraged ISAO participation, additional ISAOs specific to the medical device space are emerging:
  - Medical Device Vulnerability Intelligence Program for Evaluation and Response (MD-VIPER)
  - MedISAO
  - Southern California ISAO
  - Sensato ISAO / Medical Device Cybersecurity Task Force

Changes to a Device for Controlled vs. Uncontrolled Risk



Distinguishing Medical Device Recalls from Medical Device Enhancements

The Delicate Balance of Security, Privacy, and Safety



- "Everything is a priority"
- Varying risks to patient, device, clinical environment
- Different regulatory requirements
- Different prioritization depending on context of risk assessment
- Each can interfere with the other
  - Don't want anti-virus to fire during surgery
  - Security can erode privacy
- Our focus: safety and security

Scoring Real-World Vulnerabilities

- Can be difficult to determine safety impact of a technical finding
  - Safety regulations already require separation and indirect defense-in-depth
  - Fail-safe operations
- Vulnerable applications might not directly interact with physical actions
  - Depends on the functionality and work/data flow
- Traditional information technology (IT) often prioritizes integrity and confidentiality over availability
- For patient safety, availability is often extremely important
  - “You can’t reboot a patient”
- The clinical environment varies widely

Hospira LifeCare PCA3 and PCA5 Infusion Pump

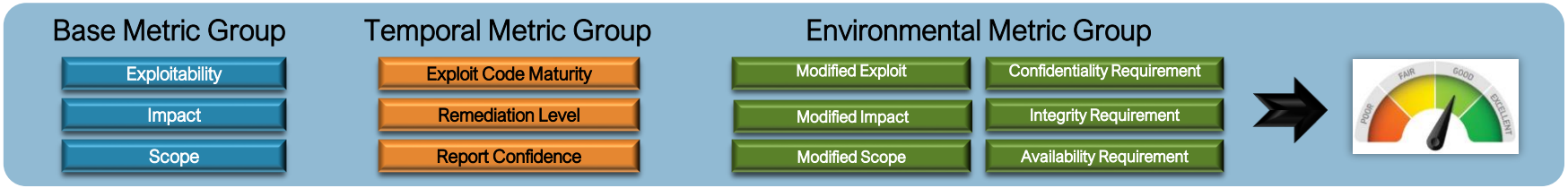
- Technical vulnerability(ies)
  - Remote telnet root access without password
  - CVSSv2: 10.0 (ICS-CERT)
- Healthcare impact
  - Change drug libraries, including min/max allowed dosage
  - (unproven?) change actual dosage delivered
- Defense-in-depth:
  - Human still needs to manually confirm dosage change
- Environmental considerations
  - Pump may be on separate, “trusted” network
  - The vulnerable interface might not even be in use
- Scoring implications
  - In a hospital performing due diligence, risk may be minimal
- References
  - ICS-CERT Advisory: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B
  - FDA Safety Communication: https://www.fda.gov/safety/medwatch/safetyinformation/safetyalertsforhumanmedicalproducts/ucm446828.htm

Image from: https://www.hospira.com/en/products_and_services/infusion_pumps/Lifecare

Desired Features of a Health Care Scoring Method

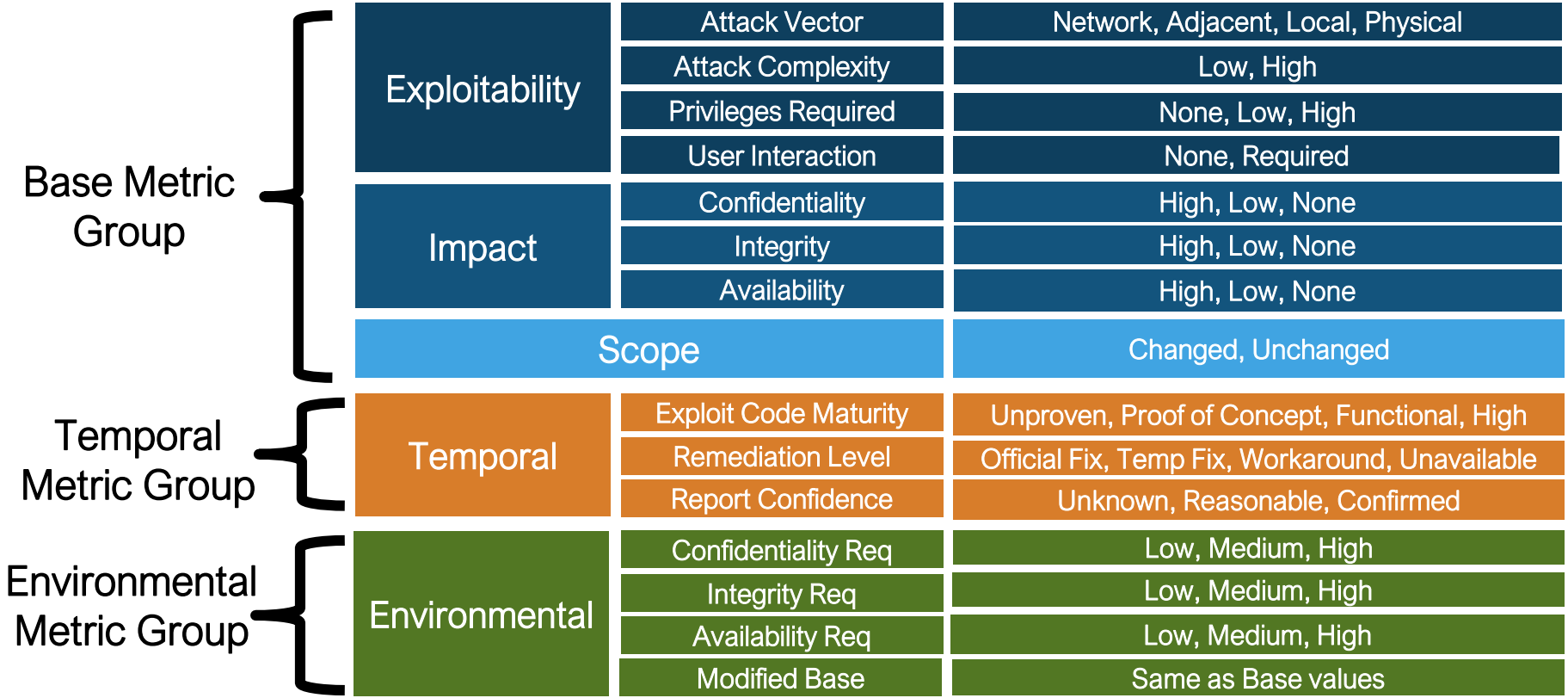
- Minimal complexity
- Usable by – and meaningful to – healthcare practitioners
- Accepted by diverse stakeholders
  - Manufacturers, hospitals, security researchers, patients, regulators
- Flexible for different clinical environments
- Flexible for different device classes
- Repeatable (different people come up with same score)
- Validated
- Provide common “language” for centering discussion and keeping disagreements focused

Common Vulnerability Scoring System (CVSS)



- **CVSS is an open framework developed by the Forum of Incident Response and Security Teams (FIRST) for communicating the characteristics and severity of software vulnerabilities**
  - Base Metric Group: vulnerability's intrinsic qualities
  - Temporal Metric Group: vulnerability's characteristics that change over time
  - Environmental Metric Group: vulnerability's characteristics unique to a user's environment.
- **Each vector element is assigned a value and a single score is computed as a weighted sum of those values**

CVSS Version 3.0



Approach

- Established a cross-stakeholder working group: medical device manufacturers, healthcare delivery organizations (HDOs), cybersecurity researchers, FIRST CVSS Special Interest Group, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), FDA
- Reviewed how some manufacturers and healthcare delivery organizations currently use CVSS
  - Concluded that CVSS is a suitable scoring system, but requires better guidance for use in healthcare settings
- Developed draft rubric through a series of telcons and email
- Conducted initial exercises to validate approach
- Submitted a proposal to FDA to qualify as a Medical Device Development Tool

CVSS Supplemental Rubric and Extended Vector

- The rubric is structured as a series of questions at various decision points for each vector element, and includes
  - Customized, HDO-specific guidance that is not included in the original specification
  - Device-specific examples
  - Discussion of difficulties in (1) repeatability of the rubric and/or (2) conformance to the spirit of the original CVSS v3 specification
  - Consideration of many perspectives that would be relevant to a medical device manufacturer or an HDO, including (1) patient safety, (2) patient/clinician privacy, and (3) cybersecurity risk from an enterprise vulnerability-management perspective

Rubric: Exploitability (Attack Vector)

No: Q3 (XAVW). Is the communication over a wireless channel?

- **Yes: Q4 (XAVR). Is the range approximately 10 feet or less?**
  - **Yes: AV = "L" (Local).** Attacker is physically close to the victim or target, and is presumed to have implied authorization, using short-range communications such as:
    - Bluetooth LE
    - Zigbee
    - Inductive communication
    - Near Field Communications (NFC)
  - **No: AV = "A" (Adjacent).** Attacker is on wireless channel with a relatively wide range.
    - 802.11b
    - Bluetooth

Rubric: Impact (Integrity)

Action 1: Determine if the attacker can modify any data or functionality that may be considered sensitive, restricted, or important by the HDO, patients, clinicians, or other caretakers? For each type of data listed, identify whether the attacker can modify All, Some, or None of the data. Answer every question.

Q1: Can attacker modify any data or functionality of type: PHI or PII?

Q2: Can attacker modify any data or functionality of type: Related to Diagnosis or Monitoring?

Q3: Can attac
therapy?

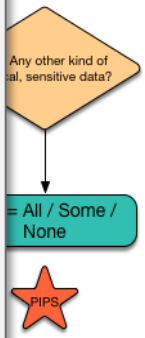
Q4: Can attac
workflow?

Q5: Can attac
system or sys

Q6: Can attac
sensitive data?

Q7 (XIA): Is "All" the answer for at least one of Q1-Q6?

- **Yes: I = "H" (High)**
- **No:**
  - **Q8 (XIM): Is "Some" the answer for at least one of Q1-Q6?**
    - **Yes: I = "L" (Low)**
    - **No: I = "N" (None)**



Medical Device Development Tool (MDDT)*

- MDDTs are scientifically validated tools that can "facilitate the scientific evaluation and assessment of a medical device by providing a more efficient and predictable means for collecting the necessary information to make regulatory assessments."
- Three tool types: clinical outcome assessment, biomarker test, nonclinical assessment model
- Qualification package
  - Description of the tool
  - Context of use
  - Strength of evidence
  - Assessment of advantages and disadvantages of qualifying the tool

*For information on FDA's MDDT program, see http://www.fda.gov/MedicalDevices/ScienceandResearch/MedicalDeviceDevelopmentToolsMDDT/

Initial Evidence Gathering Exercises

- Conducted exercises with two medical device manufacturers who use CVSS internally
- Provided scenarios of vulnerabilities – actual vulnerabilities in their own devices and public vulnerabilities in similar device
- Scored vulnerabilities using their own process and then using the rubric
- Conducted a qualitative assessment of the exercise
  - Manufacturers believed the rubric made the scoring more consistent
  - Provided confidence in our ability to gather evidence to validate the rubric

Plan to Gather Additional Evidence

- Recruit additional manufacturers
  - Assess consistency and repeatability by comparing scoring by multiple teams at each manufacturer
  - Assess accuracy and usability by comparing scoring with rubric and without rubric
- Ask ICS-CERT to rescore vulnerabilities with rubric and provide a subject matter expert assessment of using the rubric

Summary

- Implement a proactive, comprehensive risk management program
  - Apply NIST's voluntary "Framework for Improving Critical Infrastructure Cybersecurity"
  - Establish and communicate processes for vulnerability intake and handling
  - Adopt a coordinated disclosure policy and practice
  - Improve vulnerability assessment with CVSS – provide greater consistency and communication among stakeholders
  - Deploy mitigations that address cybersecurity risk early & prior to exploitation
- Engage in collaborative information sharing for cyber vulnerabilities and threats

Questions

Seth Carmody, FDA CDRH
Seth.Carmody@fda.hhs.gov

Penny Chase, MITRE
pc@mitre.org

The FDA has engaged the Centers for Medicare & Medicaid Services (CMS) Alliance to Modernize Healthcare (CAMH) Federally Funded Research and Development Center (FFRDC), operated by The MITRE Corporation (MITRE), to support FDA's medical device cybersecurity strategy.