RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PS-W01

Safety Implications of Medical Device Cybersecurity

Suzanne B. Schwartz, MD, MBA

Director, Office of Strategic Partnerships & Technology Innovation
Food and Drug Administration
suzanne.schwartz@fda.hhs.gov

Margie Zuk

Senior Principal Cybersecurity Engineer
The MITRE Corporation
mmz@mitre.org

The products we regulate…

Bottom Line Up Front (BLUF)

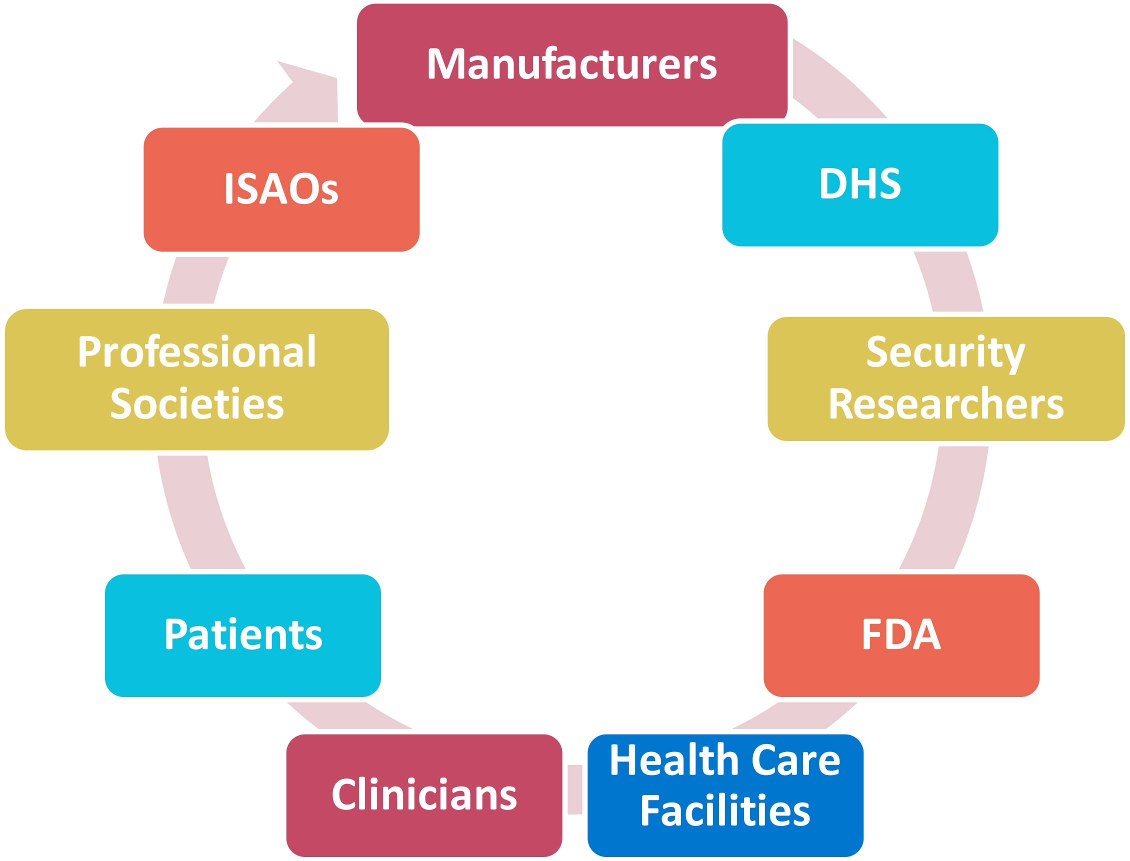
- *"Whole of community"* approach: Collaboration is key
- Security spans across the total product lifecycle
- Impact on critical infrastructure within and across sectors
- Shifting the mindset:
  - Consider scenarios beyond "intended use"
  - Integrate threat modeling
  - Beware of using probabilistic determinations—these can yield a false sense of security (avoid 'likelihood')
- Foster culture and create incentives that encourage proactive behavior, *especially for information-sharing*
- Major strides made AND acceleration necessary

Framing the Issue

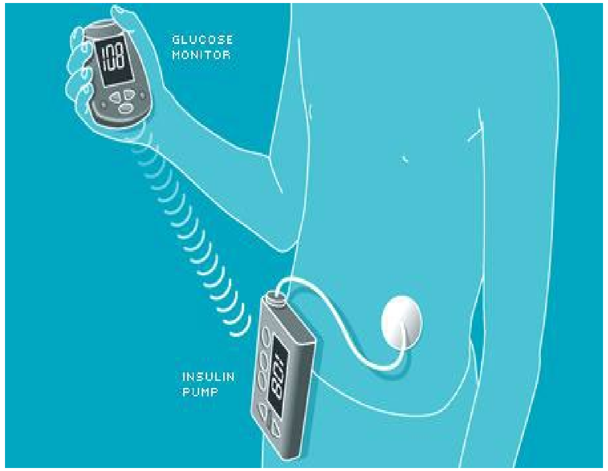
- Connected medical devices, like all other computer systems, incorporate software that are vulnerable to threats
- We are aware of cybersecurity vulnerabilities and incidents that have directly impacted medical devices or hospital network operations
- When medical device vulnerabilities are not addressed and remediated, they can be exploited which can result in:
  - patient harm
  - serve as access points for entry into healthcare delivery organization (HDO) networks
- May lead to compromise of *confidentiality*, *integrity*, and *availability*

Shared Responsibility

External Stakeholders



Medical Device Cybersecurity Background



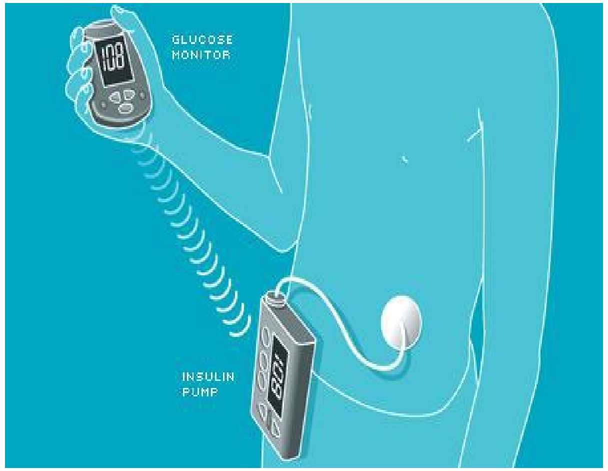
MEDICAL DEVICES

- Contain configurable embedded computer systems
- Increasingly interconnected
- Wirelessly connected
- Legacy devices

USE ENVIRONMENT

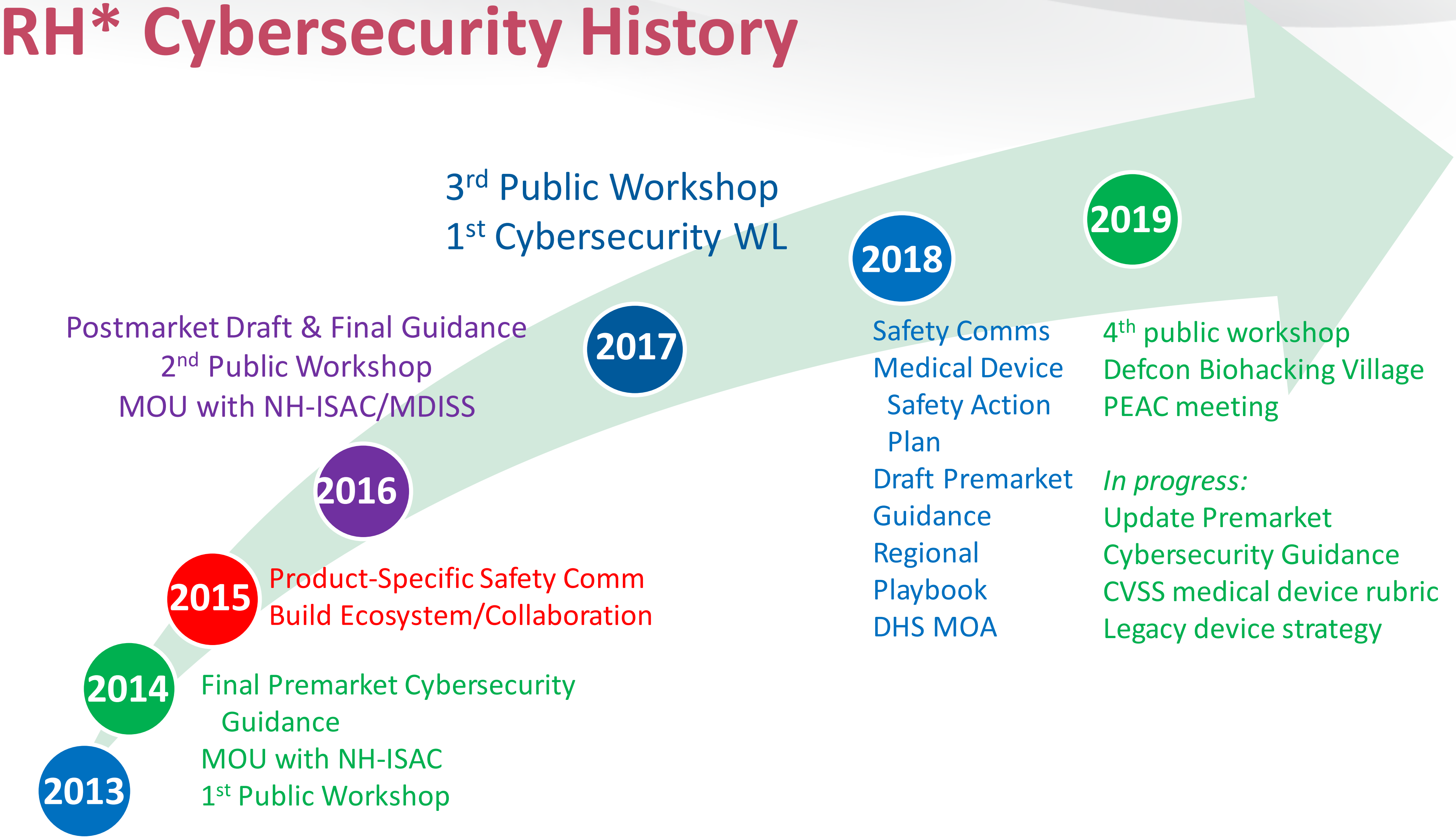
- Varied responsibilities for purchase, installation and maintenance of medical devices, often silo-ed
- Variable control over what is placed on the network
- Inconsistent training and education on security risks

Medical Device Vulnerabilities



- Network-connected medical devices infected or disabled by malware
- Malware on hospital computers, smartphones/tablets, and other wireless mobile devices used to access patient data, monitoring systems, and implanted patient devices
- Uncontrolled distribution of passwords
- Failure to provide timely security software updates and patches
- Security vulnerabilities in the off-the-shelf software that is designed to prevent unauthorized device or network access

CDRH* Cybersecurity History



2013

Executive Orders

2014

Final Premarket Cybersecurity Guidance

MOU with NH-ISAC

1st Public Workshop

2015

Product-Specific Safety Comm

Build Ecosystem/Collaboration

2016

Postmarket Draft & Final Guidance

2nd Public Workshop

MOU with NH-ISAC/MDISS

2017

3rd Public Workshop

1st Cybersecurity WL

2018

Safety Comms

Medical Device Safety Action Plan

Draft Premarket Guidance

Regional Playbook

DHS MOA

2019

4th public workshop

Defcon Biohacking Village

PEAC meeting

In progress:

Update Premarket Cybersecurity Guidance

CVSS medical device rubric

Legacy device strategy

*Center for Devices and Radiological Health

FDA

MITRE

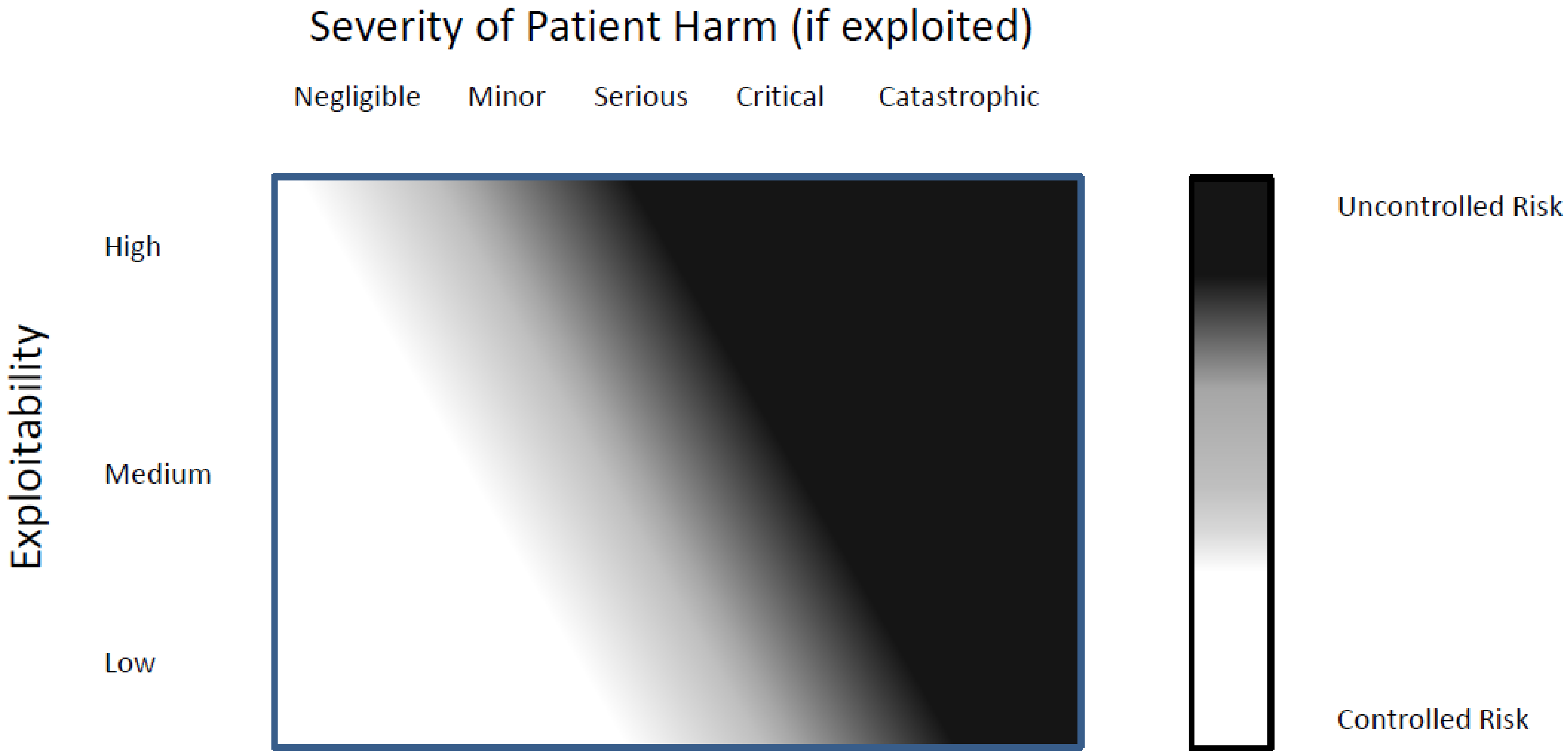
Key Principles of FDA Premarket Cybersecurity Guidance

- Shared responsibility between stakeholders, including healthcare facilities, patients, providers, and manufacturers of medical devices
- Address cybersecurity during the design and development of the medical device
- Establish design inputs for devices 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



Lessons Learned—Evolving Our Thinking

- Coordinated vs. non -coordinated disclosure of device vulnerabilities
  - Ability to get to ground truth as fast as possible so that mitigations can be proactively communicated and executed in a timely manner
    - JnJ Animas Insulin Pump
  - Non-coordinated disclosure results in delayed assessments, communications, and mitigations
    - St Jude/Abbott pacemakers and ICDs
- Impact on Healthcare and Public Health critical infrastructure and potential disruption of clinical care
  - Patching operating system is not routine with safety-critical systems
    - WannaCry Global Cyber Attack (May 2017)
    - Petya/notPetya (July 2017)
  - Delays in diagnosis/treatment intervention can result in patient harm too
- Potential for remote, multi -patient (i.e., scaled) attack of highest concern for harm

Medical Device Safety Action Plan: *Advancing Medical Device Cybersecurity*

- Update 2014 premarket guidance
- Explore the development of a CyberMed (Expert) Safety Analysis Board
- Consider seeking additional premarket and postmarket authorities to:
  - Require that firms build capabilities to update and patch device security into a product’s design and to include appropriate data supporting this capability in premarket submissions to FDA for review
  - Require firms to develop a “Software Bill of Materials” (SBOM) and to share with customers
  - Require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified

FDA and MITRE

- MITRE helping to advance the FDA medical device cybersecurity vision
  - Conducting a medical device cybersecurity stakeholder study
  - Developing a Common Vulnerability Scoring System (CVSS) Rubric for Healthcare
  - Developing a medical device cybersecurity incident response regional playbook
  - Conducting a medical device cybersecurity sandbox pilot
  - Validating the CyberMed Safety Analysis Board (CYMSAB) concept

Medical Device Cybersecurity Stakeholder Study

- Conducted Medical Device Stakeholder Study with over 80 organizations to identify cybersecurity gaps and challenges
  - Focused on HDOs, MDMs, and cybersecurity researchers
  - Presented results to Healthcare Industry Cybersecurity task force
  - Published article in AAMI BI&T

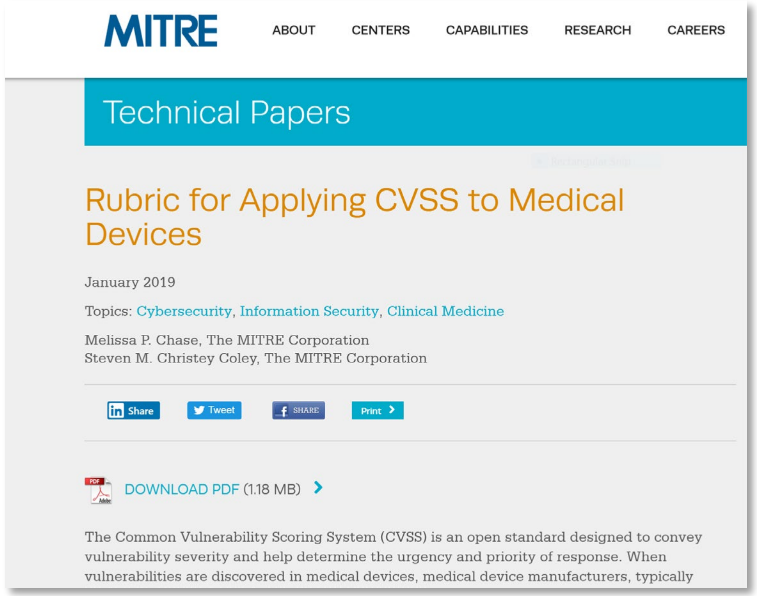
The Evolving State of Medical Device Cybersecurity

AAMI
BI&T
SEWING UP SOLUTIONS
The Role of Software Patch Management in Effective Cybersecurity

Evolving State of Medical Device Cybersecurity

Medical Device Rubric for Common Vulnerability Scoring System (CVSS)

- Established a cross-stakeholder working group: medical device manufacturers, healthcare delivery organizations (HDOs), cybersecurity researchers, FIRST CVSS Special Interest Group, DHS/CISA, FDA
- Reviewed how some manufacturers and healthcare delivery organizations currently use CVSS and concluded that CVSS is a suitable scoring system, but requires better guidance for use in healthcare settings
- Developed draft rubric with working group input/feedback
- Conducted pilots with manufacturers to validate approach
- Submitted a qualification package to FDA to qualify rubric as a Medical Device Development Tool (MDDT)



Technical Papers

Rubric for Applying CVSS to Medical Devices

January 2019

Topics: Cybersecurity, Information Security, Clinical Medicine

Melissa P. Chase, The MITRE Corporation
Steven M. Christey Coley, The MITRE Corporation

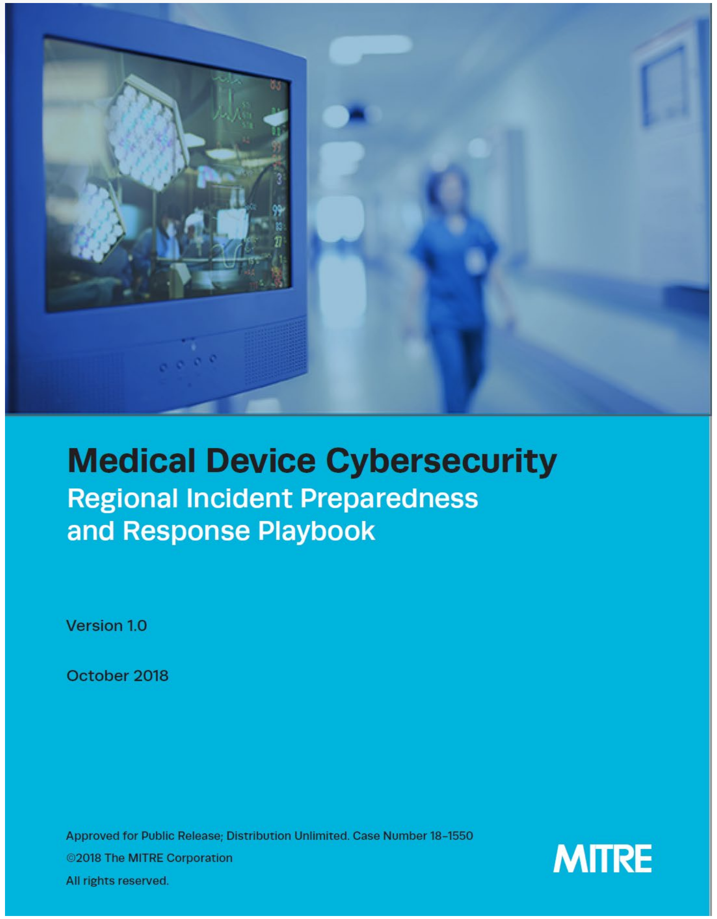
DOWNLOAD PDF (1.18 MB)

The Common Vulnerability Scoring System (CVSS) is an open standard designed to convey vulnerability severity and help determine the urgency and priority of response. When vulnerabilities are discovered in medical devices, medical device manufacturers, typically

https://www.mitre.org/md-cvss-rubric

Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook

- Published regional playbook based on input from:
  - HDO focus groups and cyber exercises
  - Boston-area workshop on WannaCry experiences
- Playbook goal: better integrate cyber, clinical and preparedness/ response activities



Medical Device Cybersecurity
Regional Incident Preparedness
and Response Playbook

Version 1.0

October 2018

Approved for Public Release; Distribution Unlimited. Case Number 18-1550
©2018 The MITRE Corporation
All rights reserved.

MITRE

https://www.mitre.org/securemed

Medical Device Cybersecurity Sandbox

- Worked with medical device manufacturers and Massachusetts General Hospital Medical Device Plug and Play (MGH MD PnP) lab to validate the concept of a cyber sandbox
- Developed clinical scenarios and use cases
- Tested the devices
- Developed and validated mitigations

CyberMed Safety Analysis Board (CYMSAB)

- Defined in Medical Device Safety Action Plan
  - a public-private partnership
  - complement existing device vulnerability coordination and response mechanisms
  - a resource for device makers and FDA
  - encompass a broad range of expertise (including hardware, software, networking, biomedical engineering, and clinical)
  - integrate critical patient safety and clinical environment dimensions into the assessment and validation of high-risk/high-impact device vulnerabilities and incidents

FDA U.S. FOOD & DRUG ADMINISTRATION
Medical Device Safety Action Plan:
Protecting Patients,
Promoting Public Health

CYMSAB (continued)

- In 2019 conducted a stakeholder study, feedback sessions, and table -top exercise to validate the CYMSAB concept and identify gaps and challenges:
  - Tailored communications for clinicians, patients and researchers
  - Vulnerability validation
  - Patch mitigation, validation, and tracking
  - Incorporating clinical risk
  - Governance and membership
  - Assisting smaller organizations to address vulnerabilities
  - Knowledge retention
  - Proactive cyber event response
  - Cyber event preparedness and coordination

Cross-Agency Collaborative Efforts

- Cybersecurity Working Groups
  - CDRH Cybersecurity Working Group coordinates and collaborates with Department colleagues, including the HHS Cybersecurity Working Group, in response to medical device cybersecurity incidents and other activities
- Healthcare Sector Coordinating Council
  - FDA contributed subject matter expertise to the Healthcare Industry Cybersecurity Task Force in development of the report issued in June 2017
  - FDA co-leads implementation of Imperative No. 2, *“Increase the security and resilience of medical devices and health IT”*
- Coordination with DHS
  - Routine coordination in which FDA provides clinical subject matter expertise to evaluate and respond to potential cybersecurity vulnerabilities and/or incidents involving medical devices

2019 Innovative Milestones

- ***#WeHeartHackers Challenge*** announced in Jan ’19, expanding x-stakeholder participation in DefCon Biohacking Village Device Hacking Lab in August ‘19:
  - Increasing medical device manufacturer (MDM) presence
  - Introducing to clinical community
  - Engaging HDOs
- Convened Patient Engagement Advisory Committee (PEAC) public meeting on medical device cybersecurity

FY2020 Targets

- Revise & Reissue Updated Cybersecurity Premarket Guidance(released as DRAFT in 2018)
- Complete CVSS clinical rubric & submit for MDDT qualification in collaboration with MITRE
- Define and operationalize Software Bill of Materials (SBOM) through multi-stakeholder engagement and cross-agency collaboration (NTIA/Dept of Commerce)
- Finalize draft International Medical Device Regulators Forum (IMDRF) guidance on total product lifecycle approach to medical device cybersecurity (FDA and Health Canada co-leads)
- Initiate Threat Modeling Bootcamp Series for device manufacturers in collaboration with MDIC
- Propose legislation that increases FDA authorities

Key Takeaways

- *"Whole of community"* approach: Collaboration is key
- Security spans across the total product lifecycle
- Impact on critical infrastructure within and across sectors
- Shifting the mindset:
  - Consider scenarios beyond "intended use"
  - Integrate threat modeling
  - Beware of using probabilistic determinations—these can yield a false sense of security
- Foster culture and create incentives that encourage proactive behavior, *especially for information-sharing*
- Major strides made AND acceleration necessary

Apply What You Have Learned Today

- This week you should visit the Medical Device Sandbox (brought by Biohacking Village) at the RSA Sandbox
- In the first three months you should learn more about medical device cybersecurity
  - What is different about operating in a clinical environment?
  - What can you learn from other sectors?
- Within six months you should:
  - Become involved in some of the Healthcare Sector Coordinating Councils Cybersecurity Working Group activities (https://healthsectorcouncil.org/)

Patient Safety depends upon Cyber Safety

FDA contacts:

Suzanne.Schwartz@fda.hhs.gov
Aftin.Ross@fda.hhs.gov
Jessica.Wilkerson@fda.hhs.gov

MITRE contacts:

Margie Zuk mmz@mitre.org
Penny Chase pc@mitre.org
Steve Christey Coley coley@mitre.org

Visit the FDA Cybersecurity Webpage:

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm