Taking Medical Device Cybersecurity to the Next Level

Session 35, August 10, 2021

Suzanne Schwartz, MD, MBA

Director, Office of Strategic Partnerships & Technology Innovation, FDA/CDRH

Margie Zuk, MS

Sr. Principal Health Cybersecurity Engineer, MITRE

HIMSS 21

FDA

MITRE

DISCLAIMER: The views and opinions expressed in this presentation are solely those of the author/presenter and do not necessarily represent any policy or position of HIMSS.

Welcome

Suzanne Schwartz

Director
Office of Strategic Partnerships & Technology Innovation
FDA/CDRH

Margie Zuk

Sr. Principal
Health Cybersecurity Engineer
MITRE

HIMSS21

#HIMSS21

Conflict of Interest

Suzanne Schwartz, MD, MBA

Has no real or apparent conflicts of interest to report.

Margie Zuk, MS

Has no real or apparent conflicts of interest to report.

Agenda

- Background and FDA Update
- Learning Objective #1: Engagements
  - International Medical Device Regulators Forum (IMDRF)
  - Health Sector Coordinating Councils (HSCC)
  - National Telecommunications and Information Administration (NTIA)
- Learning Objective #2: Vulnerability Communications
- Learning Objective #3: Threat Modeling
- Resources
- Questions?

Learning Objectives

- Describe FDA engagements with the health sector and international partners to improve the security of legacy devices and software bill of materials (SBOM)

- Identify FDA activities on developing a framework for the clear and consistent communication of medical device vulnerabilities

- Explain FDA efforts to encourage the adoption of threat modeling throughout the medical device lifecycle

2014-2020: What Have We Learned?

- Sector is maturing to be able to consider risks throughout the product lifecycle to better acknowledge and respond to reality that cybersecurity risks can arise at any time.

- Additional information about software design decisions and software supply chain would increase ability of agency/manufacturers/others to better contextualize risks.

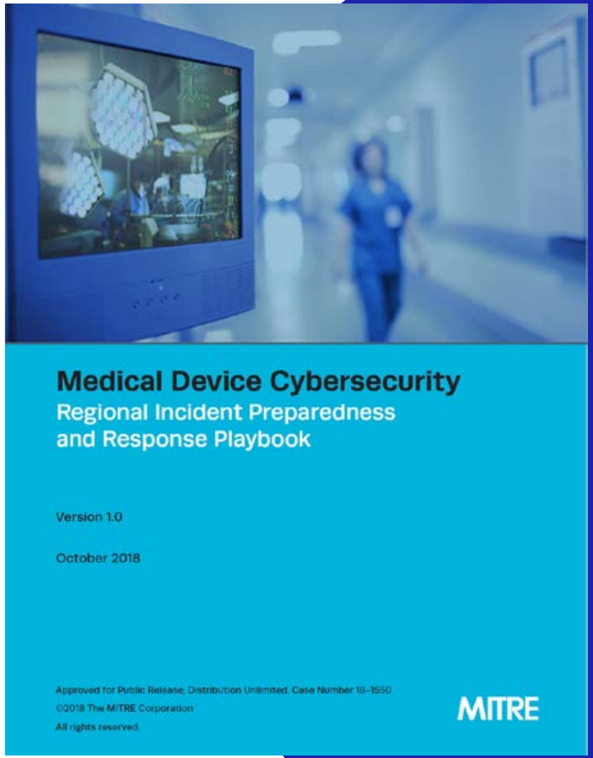
- “Building in” rather than “bolting on” security is more effective and efficient.

- Evaluation of security controls in more realistic contexts ensures more effective implementation. Stakeholders would benefit from more and better information about how to manage risks.

- Managing cybersecurity risks goes beyond simply security controls in devices—organizational infrastructure (such as CVD programs) are needed as well.

Ransomware Attacks on Hospitals

- In 2020 there were more than 560 ransomware attacks against hospitals
  - **Disrupts hospital IT systems and medical devices – can lead to extended downtimes, diversion of patients, and postponed procedures**
- Key findings from hospital interviews
  - **Develop plans and exercise with partners (incident response, disaster recovery, and continuity of operations)**
  - **Identify critical systems (EHR, Pharmacy, Radiology) and develop Business Impact Analysis**
  - **Train all staff on manual procedures (longer downtime with cyber attack)**
  - **Need to manage 3rd party (and beyond) relationships**
  - **Implement best security practices: robust backup strategy for EHR, good mail gateway, network segmentation, encryption, endpoint protection and detection response tools, penetration testing, multi-factor authentication for external access, patching, zero trust architecture**

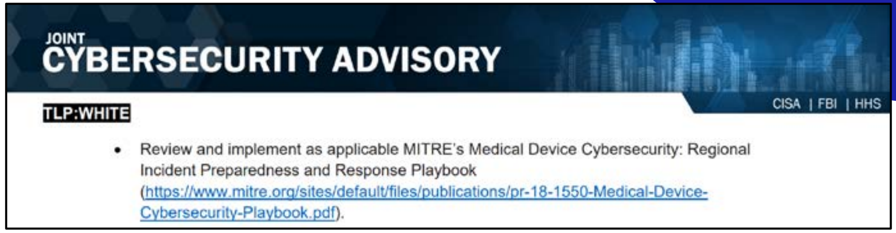


Medical Device Cybersecurity
Regional Incident Preparedness
and Response Playbook

Version 1.0

October 2018

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



JOINT
CYBERSECURITY ADVISORY

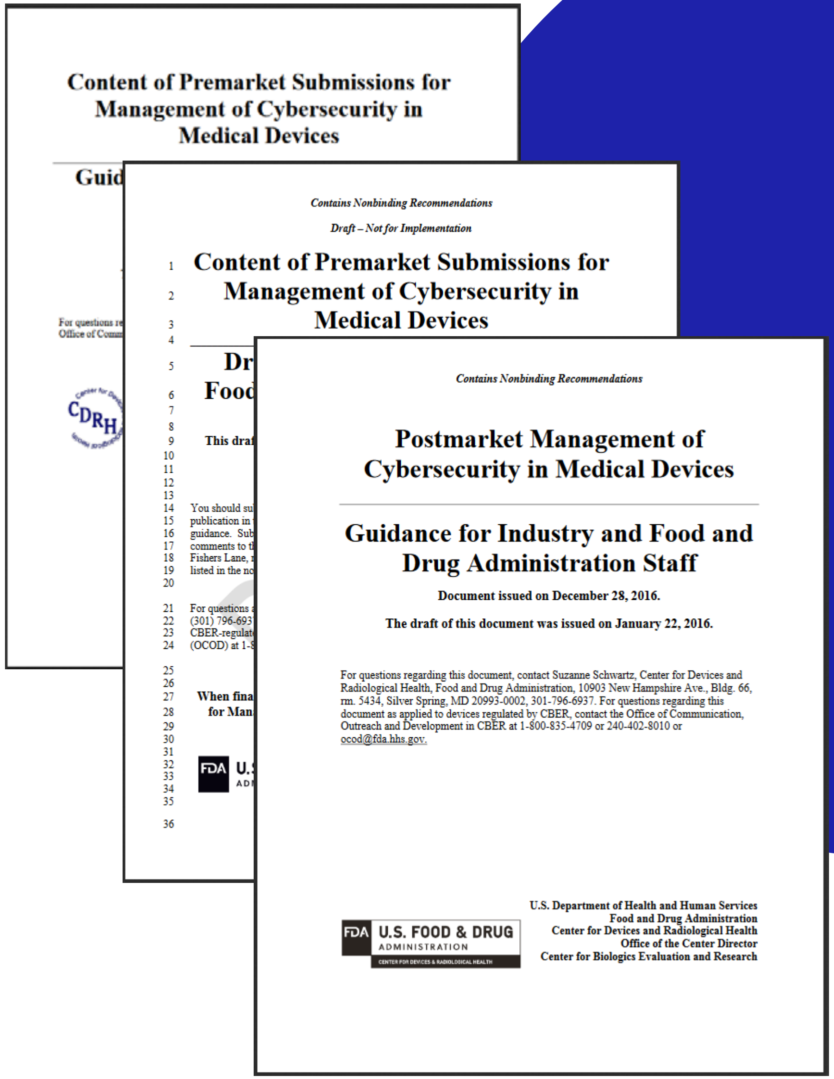
TLP:WHITE

CISA | FBI | HHS

- Review and implement as applicable MITRE's Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook (https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf).

FDA Announces Policy Through Guidances

- FDA has **statutory authority** to regulate medical devices
  - Regulations tend to be very high level
- **Guidances** articulate the Agency's current thinking on a particular subject and provide recommendations as to ***how*** industry *may* meet the regulations
- Medical device manufacturers may choose alternative measures if they can demonstrate that their quality and risk control measures meet the requirements in the regulation
- However, most manufacturers choose to comply with the recommendations provided in FDA guidances



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guid

For questions re
Office of Comm

Contains Nonbinding Recommendations

Draft – Not for Implementation

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Dr
Food

This draf

You should su
publication in
guidance. Sub
comments to t
Fishers Lane,
listed in the no

For questions
(301) 796-693
CBER-regulat
(OCOD) at 1-

When fina
for Man

Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION CENTER FOR DEVICES & RADIOLOGICAL HEALTH

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

2018 Medical Device Safety Action Plan:

Advancing Medical Device Cybersecurity

- Update 2014 premarket cybersecurity guidance
- 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 U.S. FOOD & DRUG ADMINISTRATION

Medical Device Safety Action Plan:
Protecting Patients,
Promoting Public Health

FDA Response (May 26th, 2021) to NIST Regarding EO 14028

- Underscores that cybersecurity is integral to device safety and effectiveness
- Highlights existing FDA guidance documents and international standards on the science of cybersecurity for premarket review and post-market surveillance of cybersecurity incidents and vulnerabilities
- Urges NIST and NTIA to continue and enhance their approaches to developing standards and guideline for Operational Technology cybersecurity by leveraging experts from across the public and private sectors

U.S. FOOD & DRUG ADMINISTRATION

FDA CDRH and Medical Device Cybersecurity: Response to NIST Regarding President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government (EO 14028)

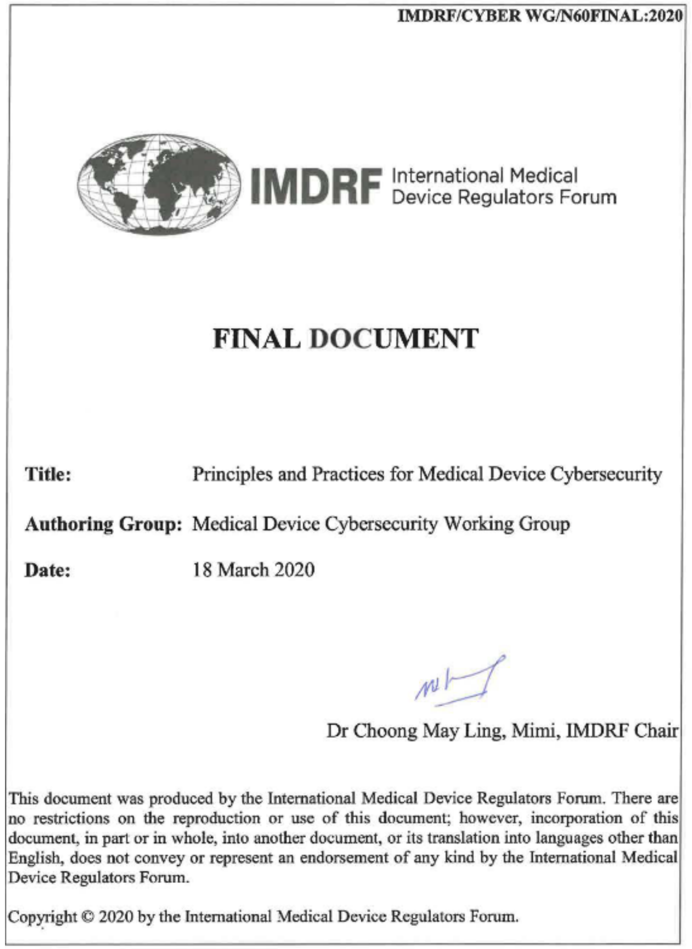
Learning Objective # 1

Describe FDA engagements

with the health sector and international partners to **improve the security of legacy devices** and software bill of materials (SBOM)

IMDRF Work

- Cybersecurity is a global issue – cybersecurity threats do not respect national borders
  - **FDA participates in the International Medical Device Regulators Forum (IMDRF) in order to work with other national regulators on shared policy issues.**
  - **FDA co-chairs a work group focused on providing international-level guidance on cybersecurity best practices for regulated entities**
- Final Document released March 18, 2020
- "Total Product Lifecycle" Approach – Design to End of Life
- Discusses legacy devices issues, coordinated disclosure, information sharing, vulnerability management, and incident response, among others



IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

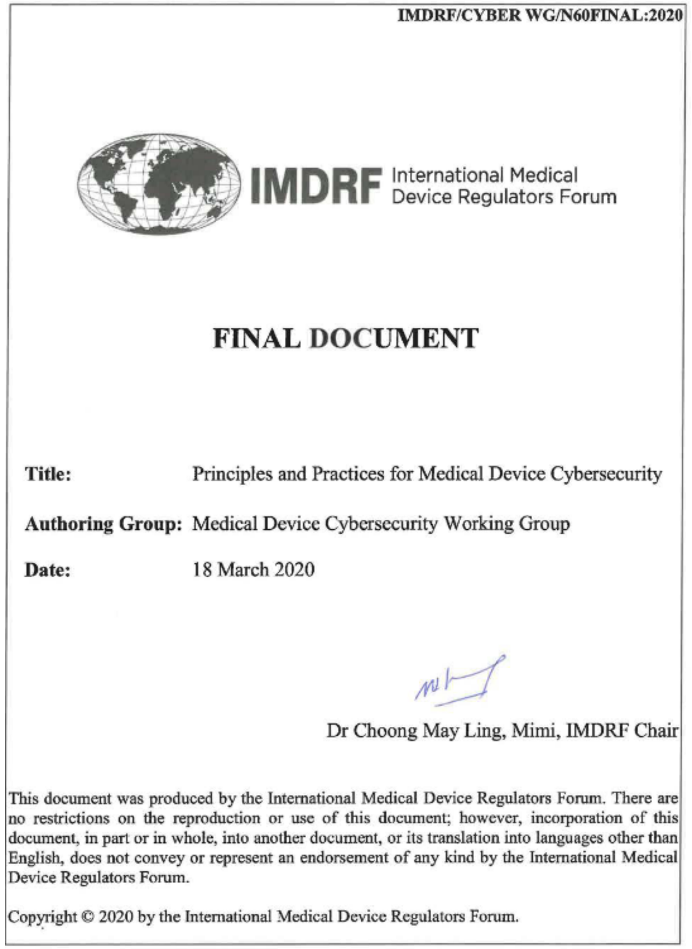
Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

IMDRF:

Software Supply Chain and SBOM

- Support for SBOM
- "The response of manufacturers to a vulnerability in a third party component should be the same as for first party vulnerabilities, namely, ongoing risk management and sharing of information with customers and users."
- "While manufacturers are unlikely to have control over the timing of resolution fora third party vulnerability (e.g., availability of an update), they are still expected to take measures to reduce risk to patients and users."



IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

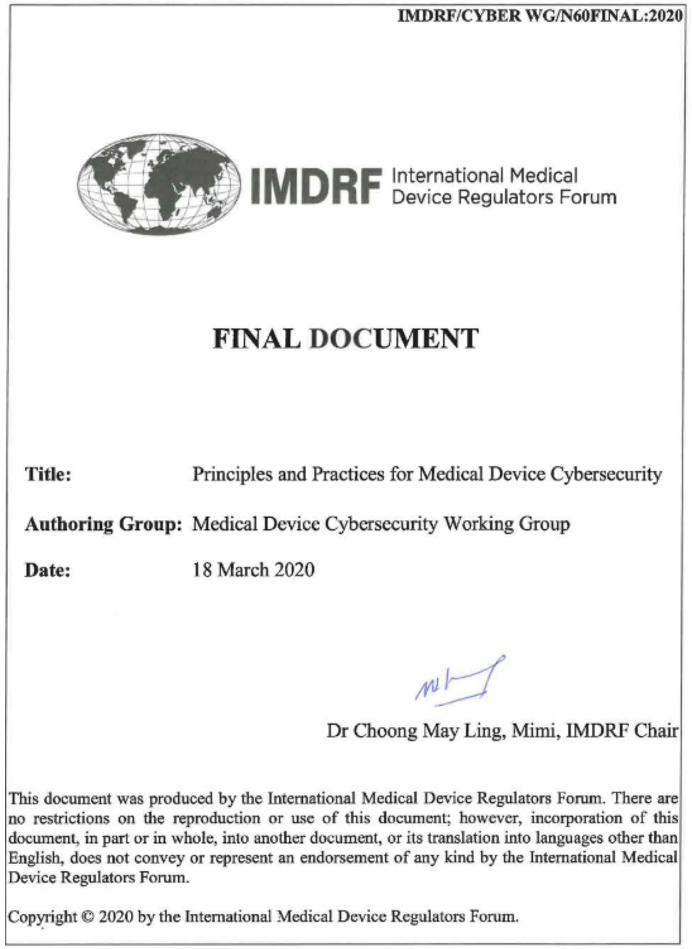
Copyright © 2020 by the International Medical Device Regulators Forum.

IMDRF:

Legacy

- Clear, multi-regulatory definition of what a "legacy" device is:

- "[M]edical devices that cannot be reasonably protected (via updates, and/or compensating controls) against current cybersecurity threats



IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

HSCC Cybersecurity Working Group:

Vulnerability Communications

- As our society has become more integrated with digital technologies, there is an evolving need for vulnerability alerts, advisories, and other communications to address a diverse set of audiences – no longer intended for only information security/cybersecurity professionals – but a broader set of users and the lay public.
- However, the language, content, and availability, among others, of these communications has yet to reflect this shift.
- Consequently, the Healthcare Sector Coordinating Council has stood up a Task Group to examine these issues.
- The Task Group's mandate is specifically to: *"Develop standardized protocols for medical device cybersecurity vulnerability communications among stakeholders"*
- Task Group is working with/leveraging FDA's existing Patient Science & Engagement (PSE) programmatic efforts, including those from the 2019 Patient Engagement Advisory Committee (PEAC) meeting.

HSCC Cybersecurity Working Group:

Legacy Device Issues

- Legacy devices create a number of challenges for robust management of cybersecurity risks in the healthcare sector.
- Consequently, the HPH Critical Infrastructure Public-Private Partnership—the Healthcare Sector Coordinating Council—has stood up a Task Group to examine these issues.
- The Task Group's mandate is specifically to: *"Develop business solutions, best practices, incentives, and policies for end-of-supported product life management and replacement of legacy medical devices."*

Software Bills of Material (SBOM)

- SBOM is a critical component of modern cybersecurity risk management
- In recognition of this, U.S. federal government began process to explore SBOM through the National Telecommunications and Information Administration (NTIA)
- With respect to "Phase 1" documents produced by NTIA process stakeholders, FDA has found:
    - **The Framing document provides a data schema that meets our needs**
    - **The "Additional Items" provision allows for growth of "baseline" SBOM**
    - **FDA intends to leverage this "additional items" provision as sector maturity w.r.t to SBOM grows**

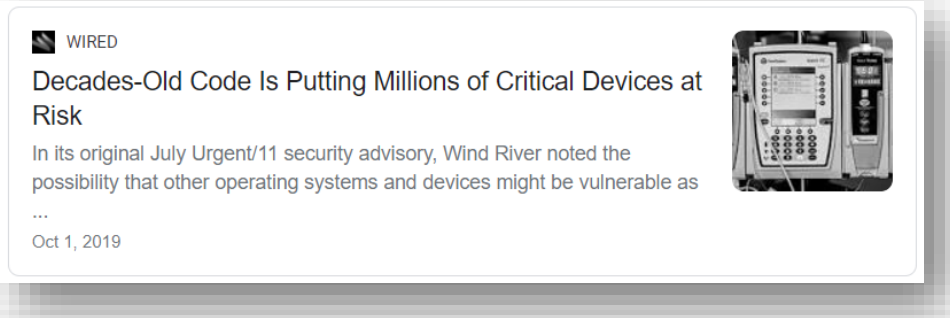
Learning Objective # 2

Identify FDA activities

on developing a framework for the **clear and consistent communication** of medical device vulnerabilities

FDA Responds to Cybersecurity Vulnerabilities

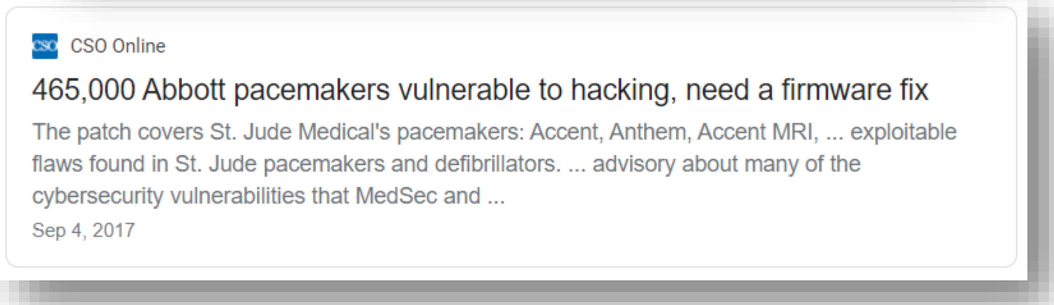
- In addition to ensuring that medical devices provide "reasonable assurance of safety and effectiveness" before they may be marketed, FDA is also responsible for ensuring such devices remain safe and effective once on the market.
- If an issue—cybersecurity or otherwise—is discovered in a medical device, the FDA takes action to:
  - **Evaluate the risk of patient harm as a result of the vulnerability**
  - **Collaborate with other appropriate parties (including the manufacturer of the device) to develop mitigations or "fixes"**
  - **Where appropriate, inform the public of the vulnerabilities.**


WIRED

Decades-Old Code Is Putting Millions of Critical Devices at Risk

In its original July Urgent/11 security advisory, Wind River noted the possibility that other operating systems and devices might be vulnerable as ...

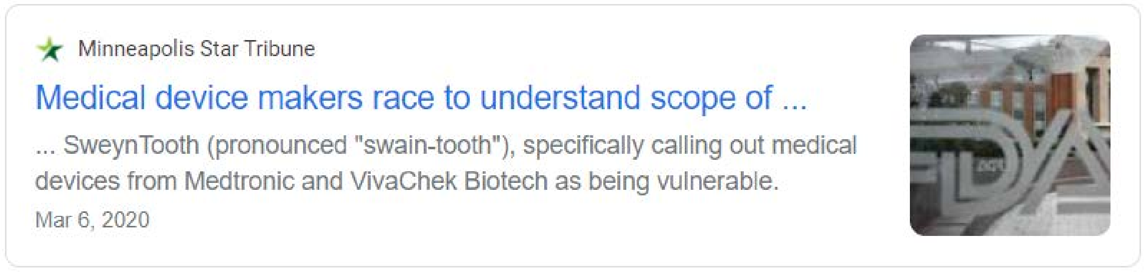
Oct 1, 2019


CSO Online

465,000 Abbott pacemakers vulnerable to hacking, need a firmware fix

The patch covers St. Jude Medical's pacemakers: Accent, Anthem, Accent MRI, ... exploitable flaws found in St. Jude pacemakers and defibrillators. ... advisory about many of the cybersecurity vulnerabilities that MedSec and ...

Sep 4, 2017


Minneapolis Star Tribune

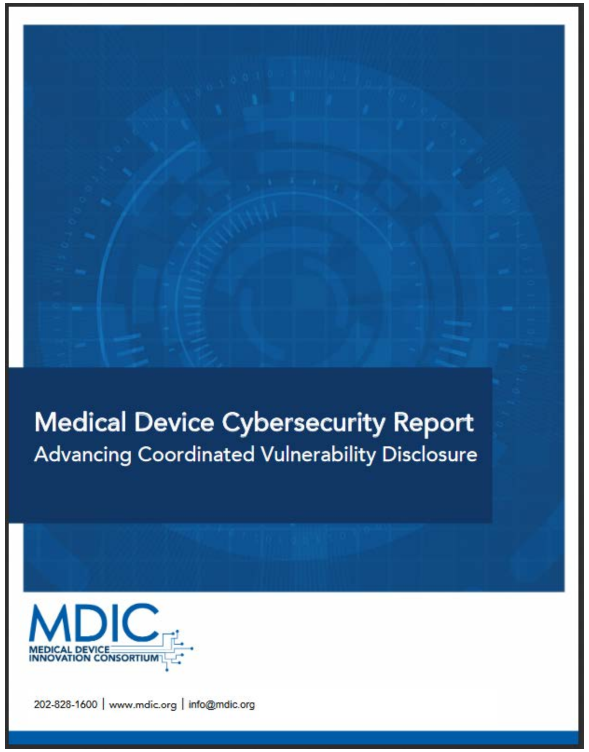
Medical device makers race to understand scope of ...

... SweynTooth (pronounced "swain-tooth"), specifically calling out medical devices from Medtronic and VivaChek Biotech as being vulnerable.

Mar 6, 2020

Coordinated Vulnerability Disclosure (CVD)

- Multiple studies have shown coordinated disclosure is a critical part of modern cybersecurity programs, given the complexity of modern information systems
- Further, FDA has observed that postmarket issues tend to reappear and/or exist in premarket as well, so CVD actions in postmarket also inform premarket



Medical Device Cybersecurity Report

Advancing Coordinated Vulnerability Disclosure

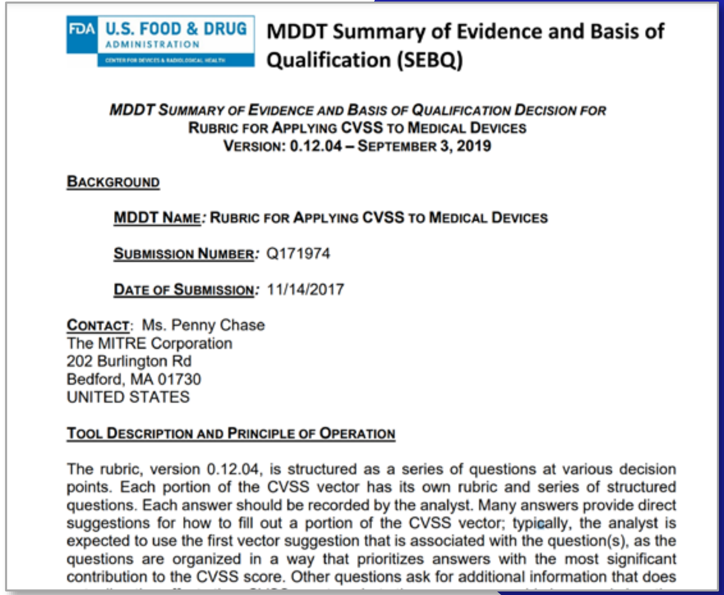
MDIC

MEDICAL DEVICE INNOVATION CONSORTIUM

202-828-1600 | www.mdic.org | info@mdic.org

CVSS Rubric Qualified as an MDDT

- **Context of use**: the evaluation and justification of patient-centric, situational impact and urgency characteristics in time-sensitive postmarket vulnerability disclosures of medical devices, when supporting the FIRST CVSS V3.0 standard. The accompanying vector string should always be published together with the score for any such evaluation.
- **Assessment of advantages / disadvantages**
  - **Reduces variability in risk assessment, "allowing lighter touch from regulators"**
  - **Facilitate culture change – vulnerability disclosures seen as an "opportunity for improvement"**
  - **Not suitable for chained attacks**
  - **Should not be used in premarket to "justify" engineering approaches to address potential vulnerability until methods to assess system cyber-resilience emerge**



FDA U.S. FOOD & DRUG ADMINISTRATION CENTER FOR DEVICES & RADIOLOGICAL HEALTH

MDDT Summary of Evidence and Basis of Qualification (SEBQ)

MDDT Summary of Evidence and Basis of Qualification Decision for
Rubric for Applying CVSS to Medical Devices
Version: 0.12.04 – September 3, 2019

Background

MDDT Name: Rubric for Applying CVSS to Medical Devices

Submission Number: Q171974

Date of Submission: 11/14/2017

Contact: Ms. Penny Chase
The MITRE Corporation
202 Burlington Rd
Bedford, MA 01730
UNITED STATES

Tool Description and Principle of Operation

The rubric, version 0.12.04, is structured as a series of questions at various decision points. Each portion of the CVSS vector has its own rubric and series of structured questions. Each answer should be recorded by the analyst. Many answers provide direct suggestions for how to fill out a portion of the CVSS vector; typically, the analyst is expected to use the first vector suggestion that is associated with the question(s), as the questions are organized in a way that prioritizes answers with the most significant contribution to the CVSS score. Other questions ask for additional information that does

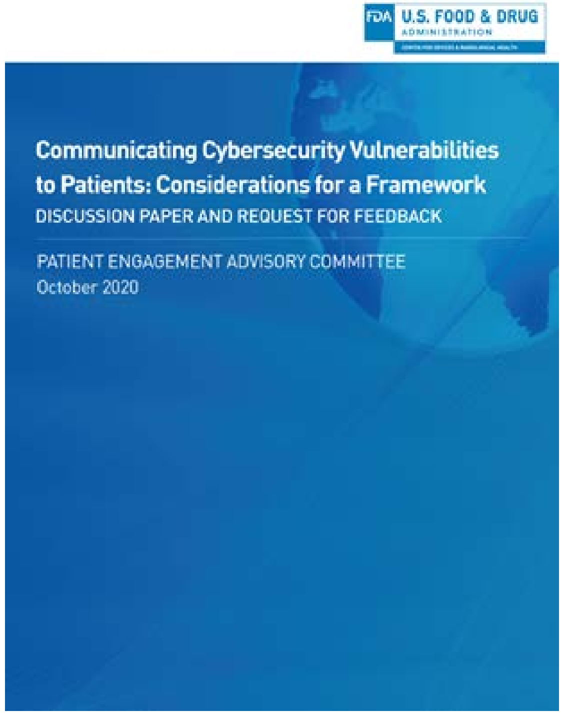
Independent Security Researchers

- FDA began working with independent security researchers to address discovered vulnerabilities within marketed medical devices.
- Independent security researchers have become a critical partner in ensuring continued improvement and maturity with respect to cybersecurity in the healthcare and public health sector.
- FDA has appreciated researchers' understanding that patient safety concerns may create different remediation timelines than those in other industries, and that they have shown a willingness to work with both the agency and the sector to address.
- FDA continues to work with researchers through initiatives like #wehearthackers and the BioHacking Village at a popular security conference.

White Paper

Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework

- In response to the PEAC's requests, FDA began exploring ways to improve cybersecurity communications with patients, culminating in a white paper that was released in October 2020.
- That white paper detailed several findings that FDA's research had revealed:
  - **Finding #1: Lead with a title that patients can personally identify with rather than industry's name for vulnerability.**
  - **Finding #2: Explain all technical jargon in plain language.**
  - **Finding #3: Simplify language and offer translation to appeal to a diverse audience.**
  - **Finding #4: Include visuals and visual cues to draw participants' attention to the main message.**
- **Looking Ahead: Development of public videos detailing cybersecurity best practices for patients and clinicians.**



FDA U.S. FOOD & DRUG ADMINISTRATION

Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework

DISCUSSION PAPER AND REQUEST FOR FEEDBACK

PATIENT ENGAGEMENT ADVISORY COMMITTEE

October 2020

Learning Objective # 3

Explain FDA efforts

to encourage the **adoption of threat modeling** throughout the medical device lifecycle

Threat Modeling

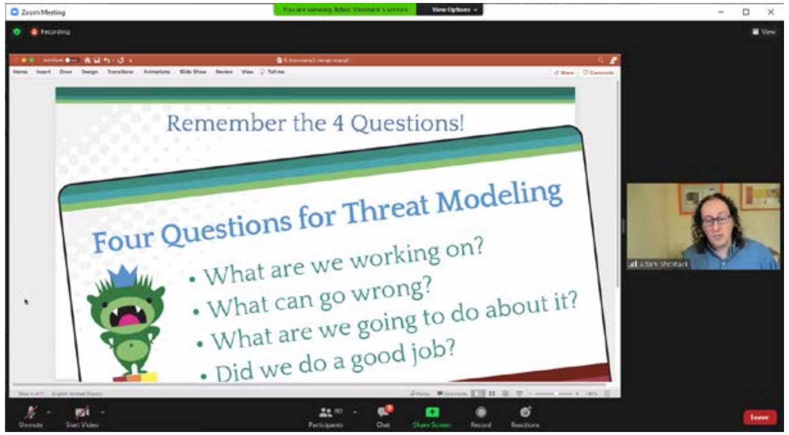
MDIC
MEDICAL DEVICE
INNOVATION CONSORTIUM

MITRE

- FDA provided funding to MDIC and MITRE to develop and host “bootcamps” to do two things:
  - **“Train the trainers” to develop individual experts within the industry who can train others to do threat modeling.**
  - **Host bootcamps to provide opportunity for “trainers” to train others within industry.**

Threat Modeling Bootcamps

- FDA is sponsoring a series of threat modeling bootcamps in collaboration with MDIC, MITRE, and Adam Shostack & Associates
  - **Initially for medical device manufacturers and FDA reviewers**
  - **Goal is to increase use of threat modeling to develop secure medical devices and enhance patient safety**
- Train the Trainer session in February 2020
- Virtual Threat Modeling Bootcamps held in August 2020 and February 2021


Remember the 4 Questions!

Four Questions for Threat Modeling

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

Threat Modeling Playbook

MITRE is developing a threat modeling playbook

- Improve consistency in threat modeling approach and documentation to support
  - Independent review with internal and external stakeholders
  - Product development teams, quality system, etc.
  - Third party pen testers, reviewers
  - Customers
- Approach
  - Leverage the learnings from threat modeling bootcamps
  - Identify current industry practices through stakeholder engagement

Threat Modeling Playbook Development

PLAYBOOK TO BE PUBLISHED IN 2021

- ✓ *Develop a generic medical device example and validate through expanded exercises at the second threat modeling bootcamp*
- ✓ *Include strategies for integrating threat modeling into business processes based on stakeholder current practices*
- ✓ *Include a range of threat modeling tools and methodologies for consideration (e.g., STRIDE,killchain, attack trees)*
- ✓ *Include additional medical device examples as time allows*

Resources

1 *IMDRF*

http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

2 *HSCC Cybersecurity Working Group*

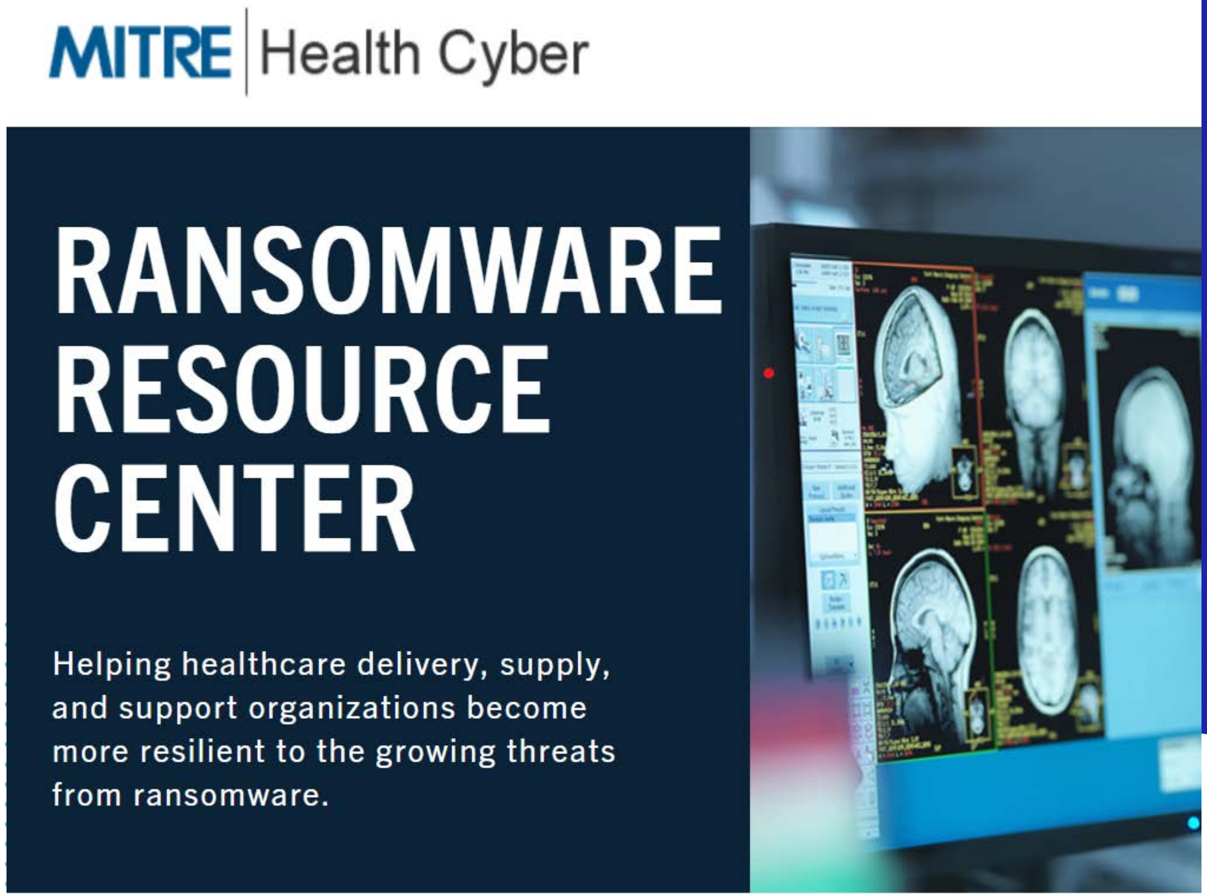
https://healthsectorcouncil.org/home/

3 *FDA*

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

Ransomware Resource Center

- MITRE developed this free resource, drawing on best practice from MITRE's own capabilities, relevant government sources, and the broader practitioner community.
- Our hope is that by curating the best available resources in one place – and providing a logical pathway for using them – we can help network defenders and IT administrators better prepare for, respond to, and recover from ransomware attacks.



MITRE | Health Cyber

RANSOMWARE RESOURCE CENTER

Helping healthcare delivery, supply, and support organizations become more resilient to the growing threats from ransomware.

https://healthcyber.mitre.org

Questions

Thank you!

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

- Margie Zuk
  - mmz@mitre.org

*Because **Cybersecurity** is a **Patient Safety Issue***