TIC COUNCIL

THE INDEPENDENT VOICE OF TRUST

TIC Council Webinar

TIC Sector and the Cyber Security of Medical Devices in North America

30 September 2020

Suzanne B. Schwartz, MD, MBA

Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health (CDRH)
U.S. Food and Drug Administration

TIC COUNCIL
Independent Voice of Trust

Michelle Jump

Global Regulatory Advisor
Medical Device Security
MedSec

TIC Sector and the Cybersecurity of Medical Devices in North America

George Strom

Director of IOT
Intertek

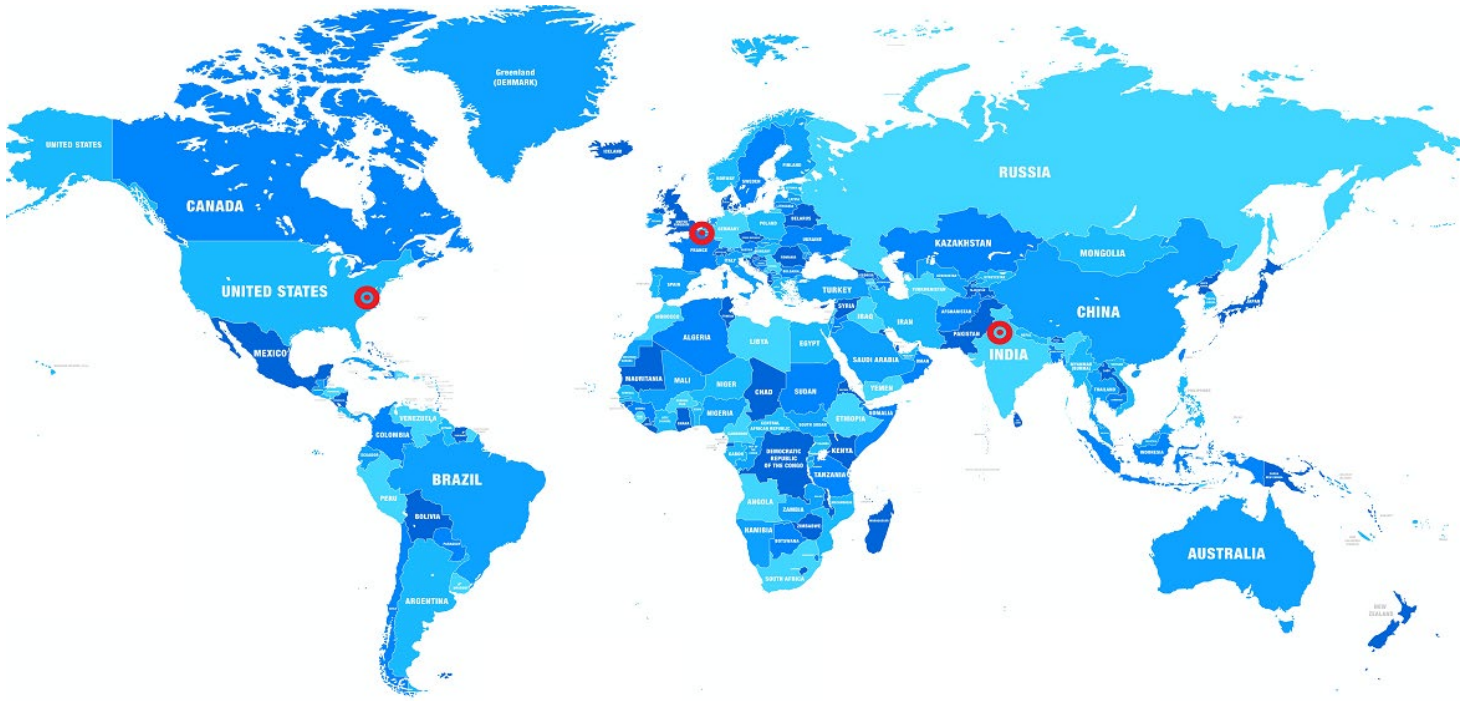
Webinar

30th September 2020 - 11:00 - 12:30 (EST)

TIC Council

The Independent Voice of Trust

- Born from the merger of IFIA and CEOC
- ~90-member companies & organizations active in more than 160 countries
- TIC Council has its head office in Brussels. It also has an office in Washington and presence in India.



TIC Council Mission

As the voice of the global independent testing, inspection and certification industry, the TIC Council engages governments and key stakeholders to advocate for effective solutions that protect the public, support innovation and facilitate trade.

The TIC Council works with its members to promote best practices in safety, quality, health, ethics and sustainability

Suzanne B. Schwartz, MD, MBA

Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health (CDRH)
U.S. Food and Drug Administration

TIC COUNCIL
Independent Voice of Trust

Michelle Jump

Global Regulatory Advisor
Medical Device Security
MedSec

TIC Sector and the Cybersecurity of Medical Devices in North America

George Strom

Director of IOT
Intertek

Webinar

30th September 2020 - 11:00 - 12:30 (EST)

Fall 2020 Update on Current FDA Medical Device Cybersecurity Work

TIC Council Webinar

Suzanne B. Schwartz, MD, MBA
Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health
US FDA
Sept 30, 2020

FDA has found 510(k) submissions to be “not substantially equivalent” (NSE) and “postmarket approval” (PMA) devices to be not approvable based on cybersecurity concerns alone.

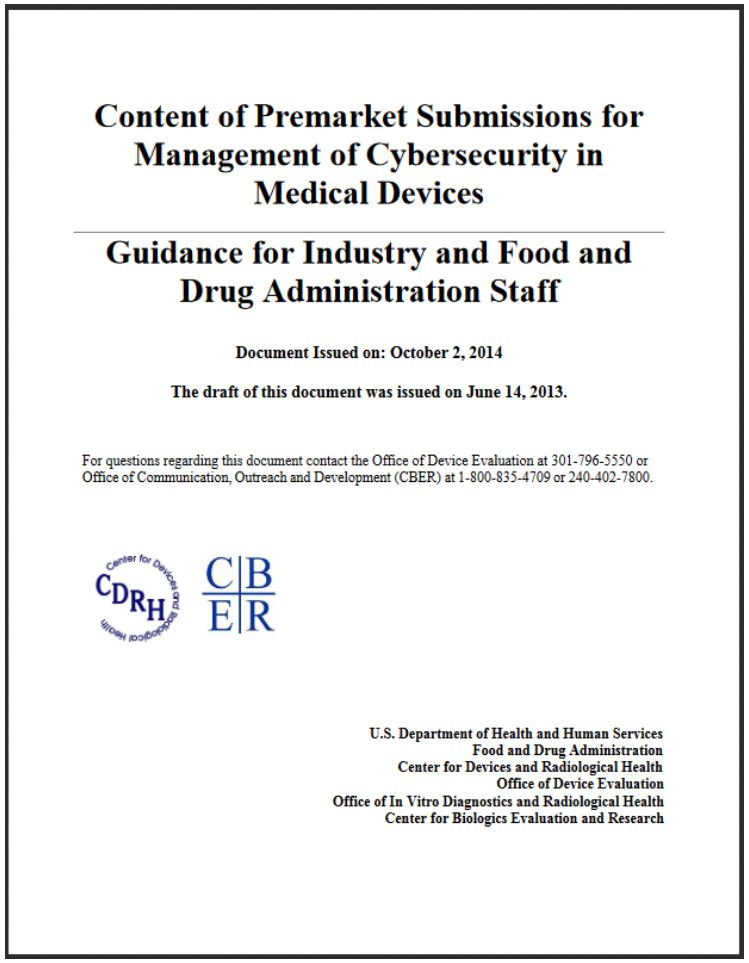
Why?

U.S. FOOD & DRUG ADMINISTRATION

Because Cybersecurity is Safety

INTERNAL AGENCY WORK

Final Guidances



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

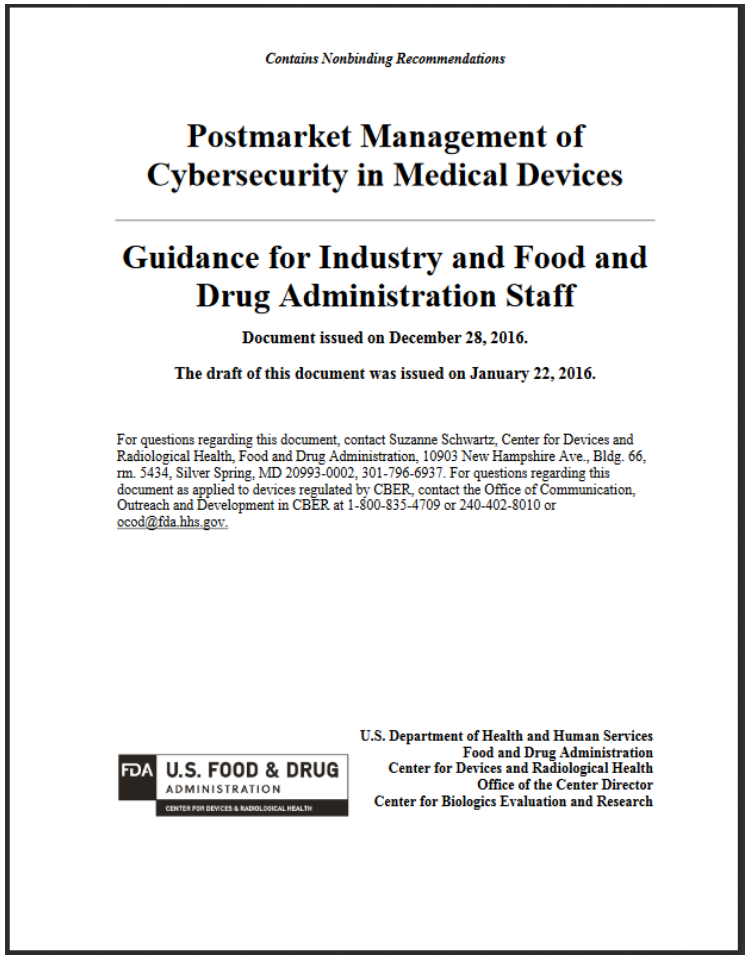
Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

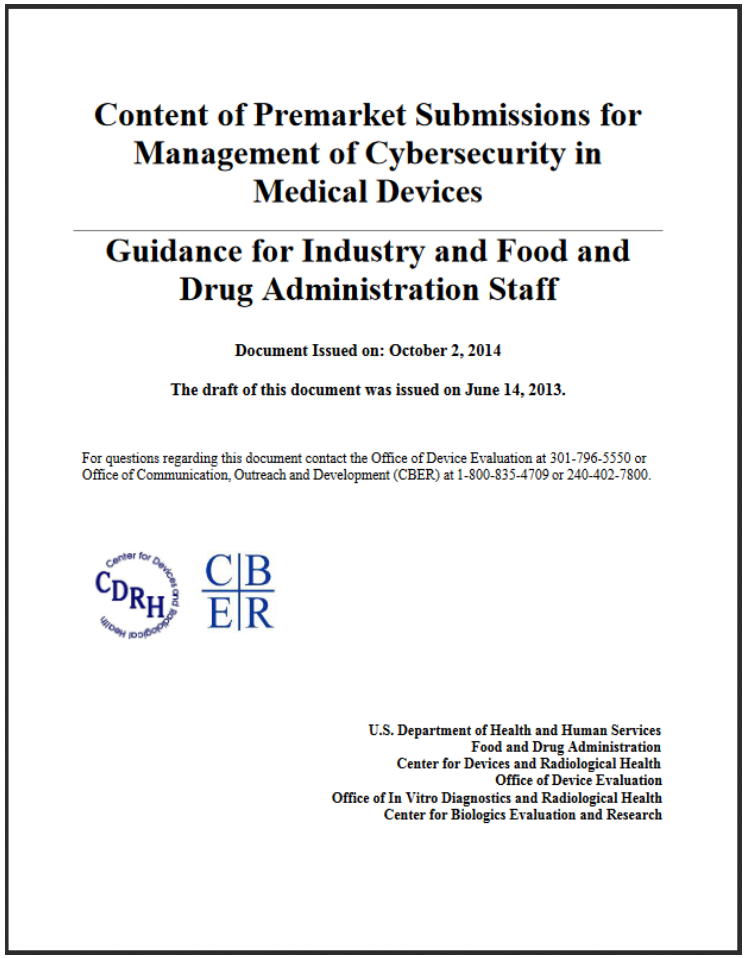
Document issued on December 28, 2016.

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.

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

2014 Premarket Guidance



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

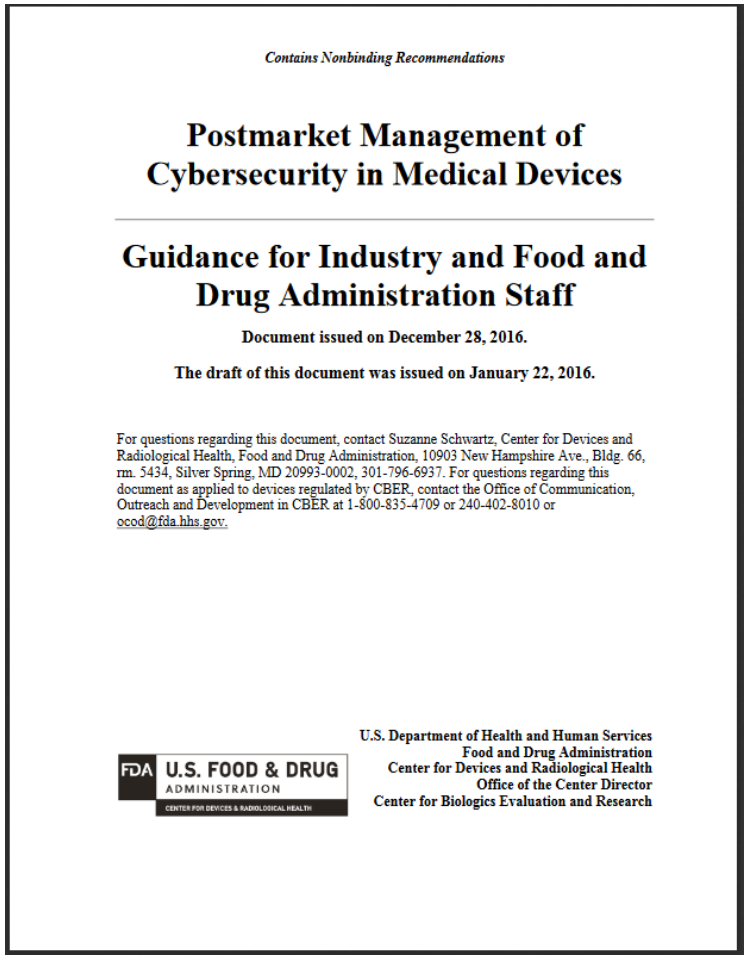
The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

- High-level guidance: allows for agency evolution alongside industry as understanding of cybersecurity throughout sector has grown
- Stressed importance of cybersecurity and risk management as part of Quality System Regulations (QSRs)
- Created a structure that allows for reviews to evolve over time, in parallel to the technology and products being evaluated
- Laid groundwork for future agency work on cybersecurity in devices

2016 Postmarket Guidance



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

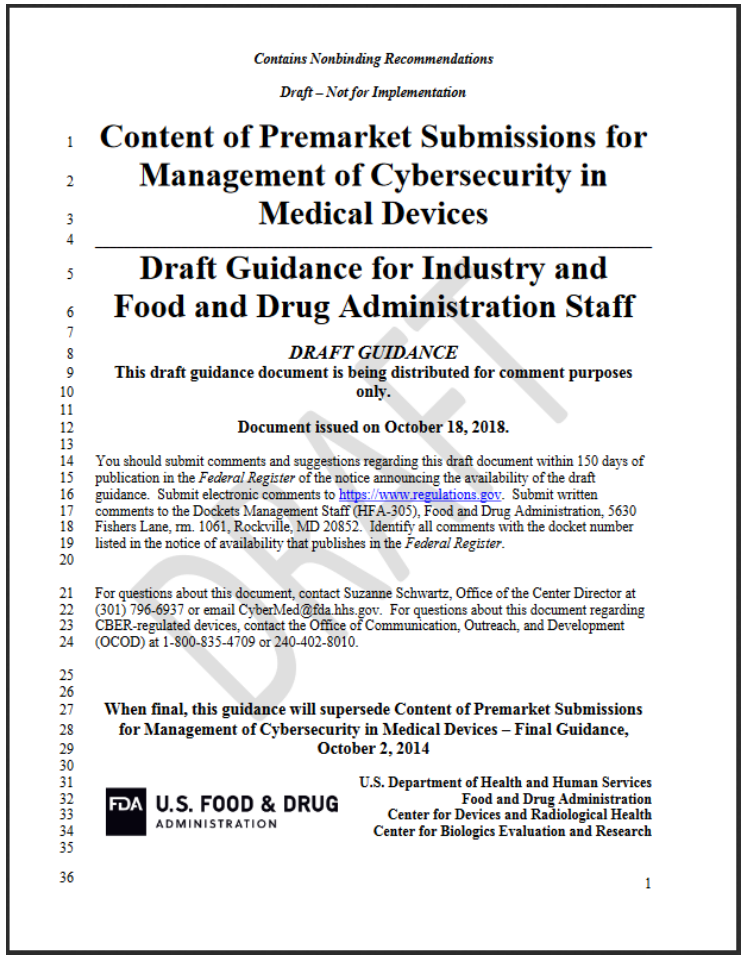
- Coordinated Vulnerability Disclosure
- Part 806 Reporting Enforcement Discretion if meeting criteria outlined in guidance
- Focus on cybersecurity risk assessments being about severity and exploitability
- Sets the stage for transferring lessons learned from postmarket to design/review decisions in premarket

2014-2018: What Have We Learned?

- HPH Sector is maturing - able to consider risks throughout the TPLC 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.

FDA has found 510(k) submissions to be “not substantially equivalent” (NSE) and “postmarket approval” (PMA) devices to be not approvable based on cybersecurity concerns alone.

2018 Draft Premarket Guidance



Contains Nonbinding Recommendations

Draft – Not for Implementation

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on October 18, 2018.

You should submit comments and suggestions regarding this draft document within 150 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions about this document, contact Suzanne Schwartz, Office of the Center Director at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

FDA U.S. FOOD & DRUG ADMINISTRATION

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

1

DRAFT

- Greater focus on criticality of security throughout the TPLC
- Includes software supply chain transparency and SBOM
- Security architecture and security control recommendations to “build in” rather than “bolt on” security
- Increased focus on security testing & introduced threat modeling
- Identification and discussion of organizational and procedural needs with respect to cybersecurity

Premarket Guidance Update re: Comments

- Better aligns with a Secure Product Development Framework (SPDF); e.g.,
  - Medical Device and Health IT Joint Security Plan (JSP)
  - ANSI/ISA 62443-4-1 Security for industrial automation and control systems
- Removed Tiers
- Cybersecurity Bill of Materials to Software Bill of Materials

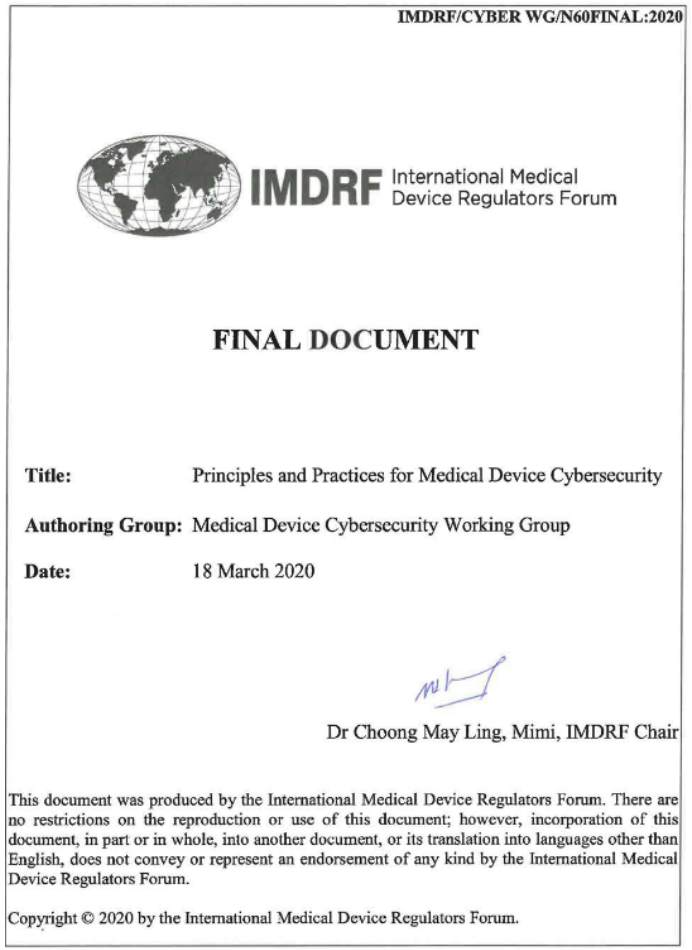
Threat Modeling

- 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.

PARTNERSHIP EFFORTS AND COLLABORATIONS

IMDRF Work

- 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

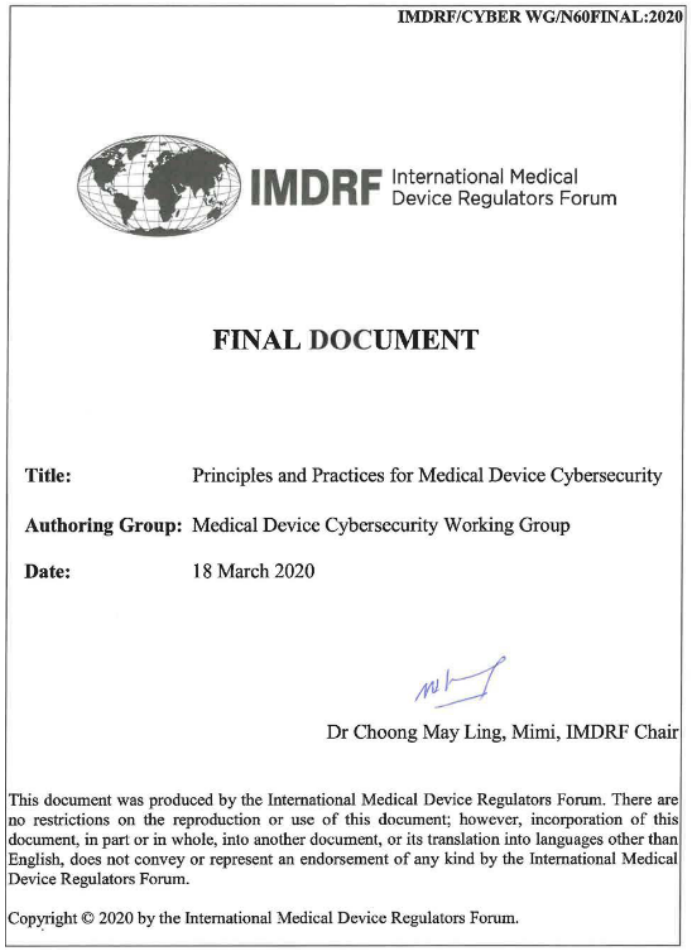
Dr Choong May Ling, Mimi, IMDRF Chair

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

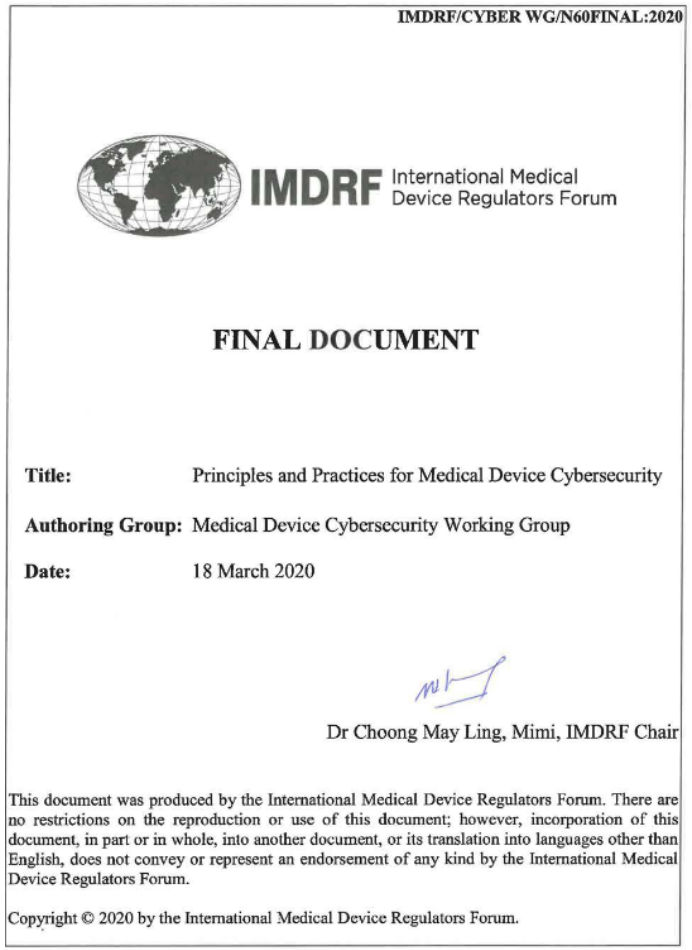
Dr Choong May Ling, Mimi, IMDRF Chair

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.

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

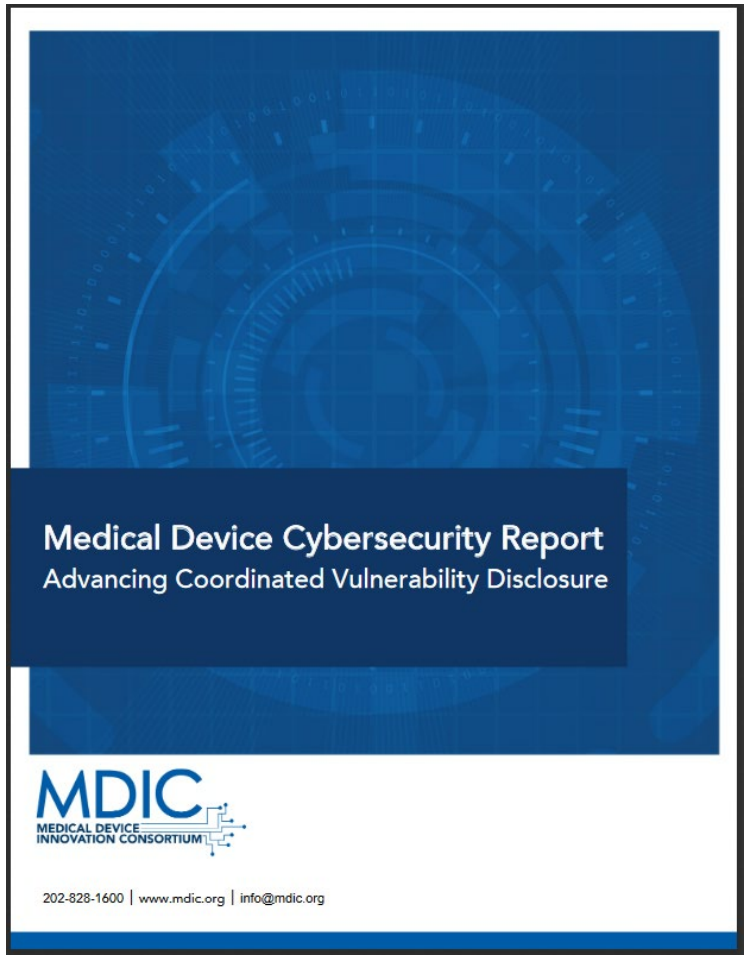
Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

Coordinated Disclosure

- 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



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

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."

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 Engagement efforts, including those from the **2019 Patient Engagement Advisory Committee** meeting.

Other Resources

- MITRE Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
- MITRE Rubric for applying CVSS to medical devices
- NTIA Coordinated Vulnerability Disclosure Reports/Documents
- FDA Off-the-Shelf Software Guidance

Wrap Up

- FDA's approach is evolving, and will continue to evolve together with the ecosystem, as medical devices are developed and deployed.
- We will continue to work both internal to the agency and externally with partners to ensure the sector has as comprehensive and as robust approaches to healthcare cybersecurity as possible.
- Why?

U.S. FOOD & DRUG ADMINISTRATION

Because Cybersecurity is Safety

Questions About Submission Process?

- Email CyberMed@fda.hhs.gov or OPEQ_Cybersecurity@fda.hhs.gov

- FDA *highly* encourages stakeholders to take advantage of Qsub process.

THANK YOU!

OCTOBER IS NATIONAL CYBERSECURITY AWARENESS MONTH

Suzanne B. Schwartz, MD, MBA

Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health (CDRH)
U.S. Food and Drug Administration

TIC COUNCIL
Independent Voice of Trust

Michelle Jump

Global Regulatory Advisor
Medical Device Security
MedSec

TIC Sector and the Cybersecurity of Medical Devices in North America

George Strom

Director of IOT
Intertek

Webinar

30th September 2020 - 11:00 - 12:30 (EST)

Global Medical Device Cybersecurity: An Industry Perspective

TIC Council Webinar

Michelle Jump

MedSec

September 30, 2020

MedSec

Agenda

Global Trends

Security Risk Management & Threat Modeling

Challenges

MedSec

Michelle Jump

Global Regulatory Advisor – Medical Device Cybersecurity
MedSec
michellejump@medsec.com

Global Trends in Medical Device Cybersecurity

Global Regulatory Guidance: Rapid pace of release

https://h-isac.org/medical-device-security-part-1-landscape-of-global-regulatory-guidance/

MedSec

Chronology

2018 & 2019 saw a rapid increase in guidance document releases

IMDRF finalized late 2019 – outlining key considerations for regulators

Many of these guidance documents are summarized in recent whitepaper co-authored by Salwa Rafee (H-ISAC) and me. <link>

YEAR	COUNTRY	DOCUMENT TITLE
2005	United States	Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (Final)
2014	United States	Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Final)
2015	Japan	Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1 (Final)
2016	United States	Postmarket Management of Cybersecurity in Medical Devices (Final)
2017	China	Medical Device Network Security Registration on Technical Review Guidance Principle (Final)
2018	Germany	Cybersecurity Requirements for Network-Connected Medical Devices
	Japan	Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1 (Final)
	Singapore	TR67: Connected Medical Device Security (Final)
	South Korea	Cybersecurity Guide for Smart Medical Service (Final)
	United States	Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Draft)
2019	Australia	Medical device cybersecurity guidance for industry (Final)
	Canada	Pre-market Requirements for Medical Device Cybersecurity (Final)
	France	Cybersecurity of Medical Devices integrating software during their lifecycle (Draft)
	Saudi Arabia	Guidance to Pre-Market Cybersecurity of Medical Devices
	IMDRF	IMDRF Principles and Practices for Medical Device Cybersecurity (Draft)
2020	IMDRF	Principles and Practices for Medical Device Cybersecurity
	European Union	MDCG 2019-16 Guidance on Cybersecurity for medical devices

Product Security Programs can be broken down into 5 Foundational Elements

1. Secure Design and Testing
2. Security Risk Management
3. Labeling and Communication
4. Vulnerability Management
5. Incident Response

This doesn't cover every individual item but gives you a solid foundation to establish a program that fits the big picture for most global expectations.

Then focus on submission expectations for the target markets

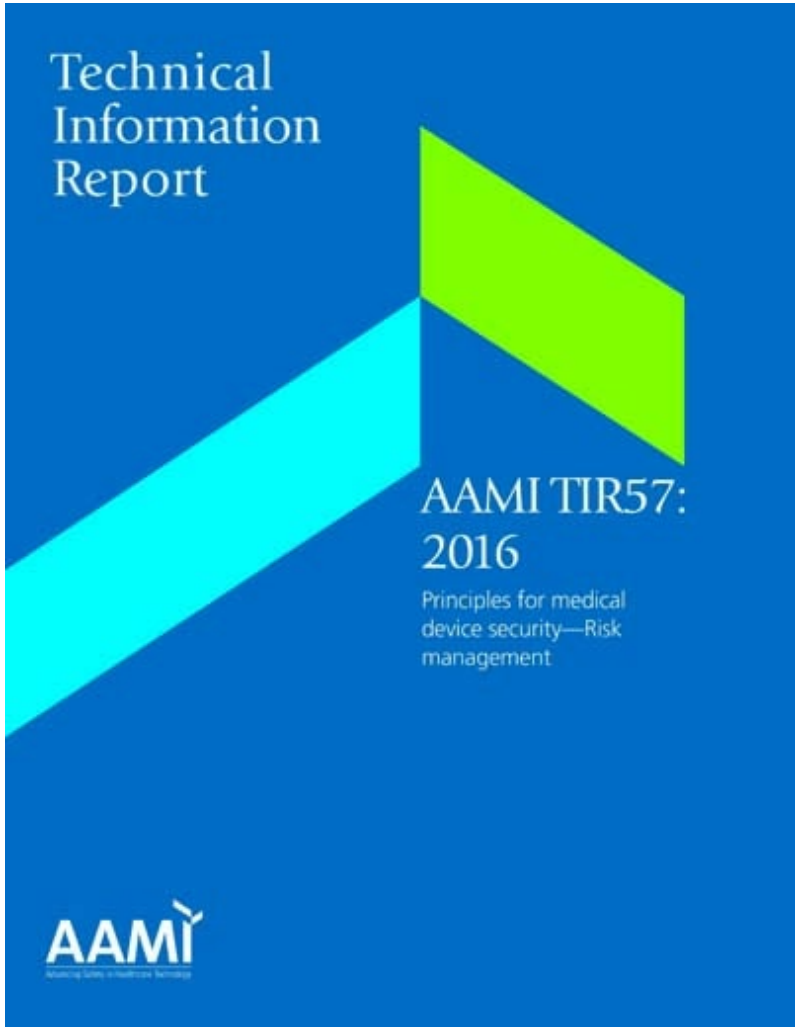
Step 1: Secure the Design

- Most guidance provides security controls and requirements to consider
- Defense-in-Depth, layered security controls
- Modularized architecture
- Testing
- Penetration testing and vulnerability analysis (UL290 as a guide)

MedSec

Step 2: Risk Management

- Risk Management is the foundation of any product security program
- AAMI TIR 57 is used as a reference in most global regulatory guidance
- Key process for deciding if and when a manufacturer must act
- Security risk management uses a different “ruler” for measuring risks as compared to ISO 14971
- Threat modeling – help identify specific threats to your system



MedSec

Step 3: Labeling and Communicate

- Strong focus for many regulators
- Demonstrates the importance of a shared responsibility
- Need to communicate:
  - Operational environment
  - System requirements
  - Security capabilities
  - Access controls and authentication
  - Patch management
  - Interfaces
  - High-level risk summary
- Security whitepapers are often useful
- Software Bill of Materials (SBOM)
- Manufacturer Disclosure Statement for Medical Device Security (link)

MedSec

Step 4: Vulnerability Management

- Vulnerabilities evolve over time
- You must monitor for these, assess, and patch if appropriate
- Also need to know what type of third-party component make up your device – source of many emerging vulnerabilities
  - Use SBOM to help this
- NTIA SBOM Phase 1 reports

  https://www.ntia.gov/SBOM
- Coordinated Vulnerability Disclosure: key communication tool

MedSec

Step 5: Incident Response

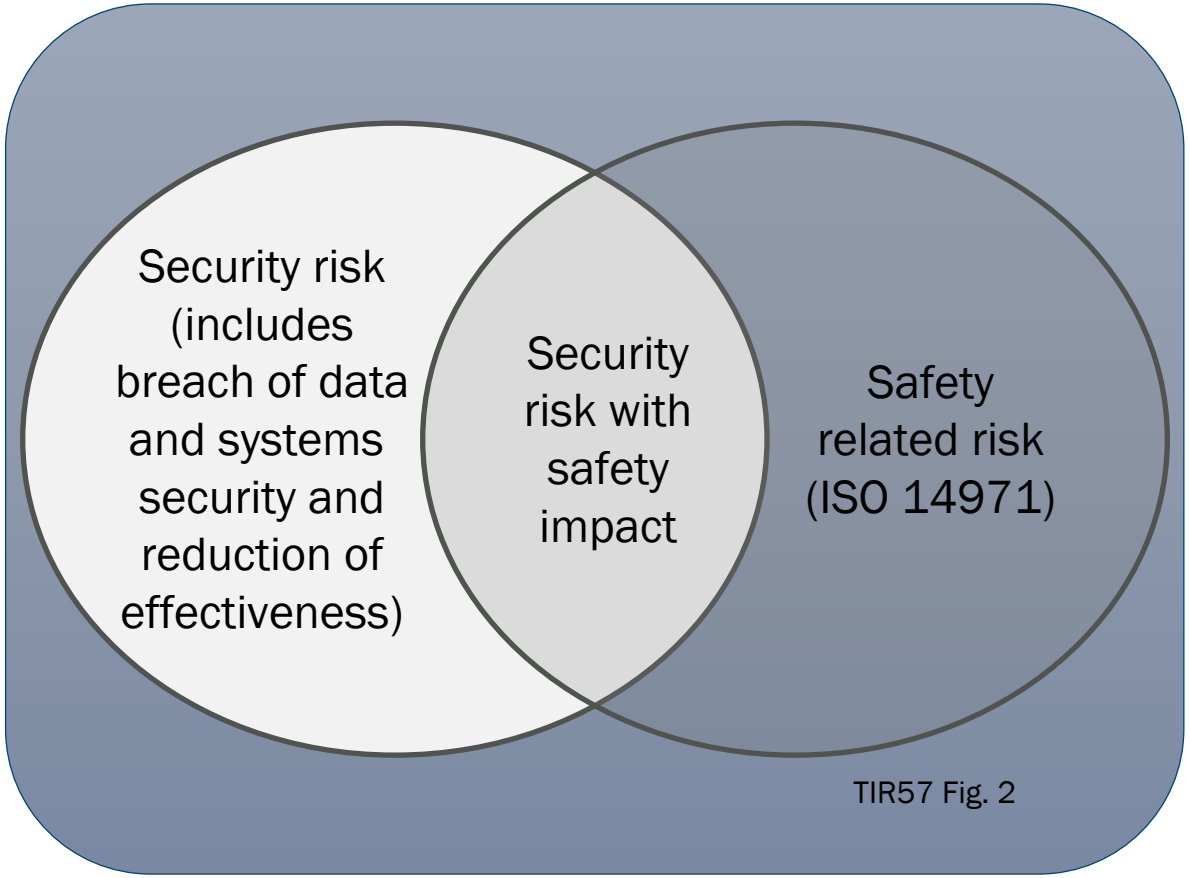
- Even with best efforts, you need to be prepared for an actual cyber attack related to your product
- Plan for a **rapid, organized response** that includes communication and recovery
- **Tabletop Exercises:** practice, practice, practice. Actual incidents are not the time to test out your process
- Often coordinated with organization's larger enterprise response plan

MedSec

Security Risk Management & Threat Modeling

Security Risk Management

- Security Risk Management is unique
- Security can impact safety but not always
- Not always apparent if it is safety related
- Severity/Occurrence often does work



- "Discovering" threats can require a different approach
- Security threats emerge differently, can rapidly expand globally, and have a human element that requires consideration

Threat-Modeling Role in Risk Management: Why do it?

Threat-modeling methods are used to create

- an abstraction of the system
- profiles of potential attackers, including their goals and methods
- a catalog of potential threats that may arise

Threat-modeling can help provide a more comprehensive and well-rounded view of threats as compared to more generic risk management methods

Threat-modeling should be performed early, with assistance of trained security professionals

MedSec

Threat Modeling Methods: STRIDE

Various methods are available for threat modeling. A common approach is to use STRIDE threat categories. Adopted my Microsoft in 2002, it is the most mature method available today. Others include DREAD, Attack Trees, & OCTAVE

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

MedSec

Challenges


Requirements
COMPLIANCE
Policies
Transparency
Terms
Law
Guideline
Regulations
Audit
Standards

Hospitals have 10-15 medical devices for each patient bed

MedSec

Medical devices are continuing to age.

Creating an issue with Legacy Devices

Becomes more difficult to patch as software components age

MedSec

Limited funds to replace aging devices.

MedSec

Thank you

MedSec

Suzanne B. Schwartz, MD, MBA

Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health (CDRH)
U.S. Food and Drug Administration

TIC COUNCIL
Independent Voice of Trust

Michelle Jump

Global Regulatory Advisor
Medical Device Security
MedSec

TIC Sector and the Cybersecurity of Medical Devices in North America

George Strom

Director of IOT
Intertek

Webinar

30th September 2020 - 11:00 - 12:30 (EST)

TIC COUNCIL

THE INDEPENDENT VOICE OF TRUST

TIC Sector and the Cyber Security of Medical Devices in North America

George Strom
Intertek - Connected World

30 September 2020

TIC SECTOR AND THE CYBER SECURITY OF MEDICAL DEVICES IN NORTH AMERICA:

1. **WHAT ARE THE MAIN CHALLENGES ON MARKET BASED ON THE TIC INDUSTRY'S EXPERIENCE?**

2. **WHAT ARE THE BEST PRACTICES MANUFACTURERES SHOULD TAKE INTO CONSIDERATION FOR MITIGATING RISKS AND ENSURING COMPLIANCE WITH CYBER SECURITY REQUIRMENTS IN NORTH AMERICA?**

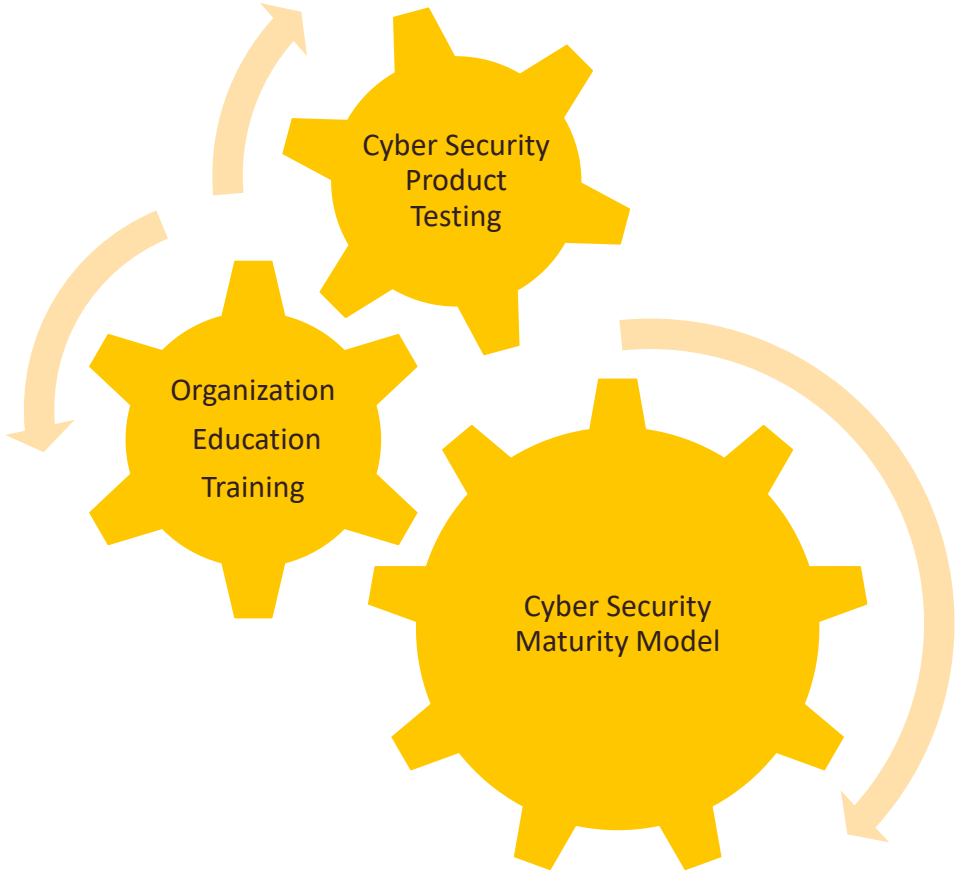
3. **CAN YOU ADDRESS THE NEED FOR VA AND PEN TESTING FOR CERTAIN CATEGORIES OF MEDICAL DEVICES, HOW TO DEAL WITH MEDICAL APPS AND CURRENT CHALLENGES?**

TIC SECTOR AND THE CYBER SECURITY OF MEDICAL DEVICES IN NORTH AMERICA:

1

WHAT ARE THE MAIN CHALLENGES ON MARKET BASED ON THE TIC INDUSTRY'S EXPERIENCE

WHAT ARE THE MAIN CHALLENGES ON MARKET BASED ON THE TIC INDUSTRY'S EXPERIENCE?



- Development of Cyber Security Model
  - Affordability
  - Budget
  - Where do I begin
  - Impact on my Organization & Product
- Regulatory Awareness
  - FDA
  - Health Canada
  - EU MDR & IVDD
- Perception
  - Budget
  - Traditional Testing (i.e Product Safety) First

WHAT ARE THE MAIN CHALLENGES ON MARKET BASED ON THE TIC INDUSTRY'S EXPERIENCE? THREAT LANDSCAPE

RISKS POSED BY INSECURE CONNECTED MEDICAL DEVICE

Access to Patient information

- Need to protect your personal information from getting into the hands of attackers

Unauthorized access to services

- Need to protect your IoT device from unauthorized access (e.g. unlocking your door)

Attacks launched from IoT

- Need to protect your IoT device from being used as a platform to attack other networks and devices

WHAT ARE THE MAIN CHALLENGES ON MARKET BASED ON THE TIC INDUSTRY'S EXPERIENCE?

Legacy Products

- Patching
- Software Upgrades
- Unsupported Software

Acquisitive Products

- What vulnerabilities are present?
- Unsupported Software

New Product Innovation:

- Security Design Consideration
- Risk Management
- Cyber Security Requirements

•What are the risks?

What is at risk if the device is compromised? The more serious the risk to patient safety, the more stringent and rigorous the security requirements should be.

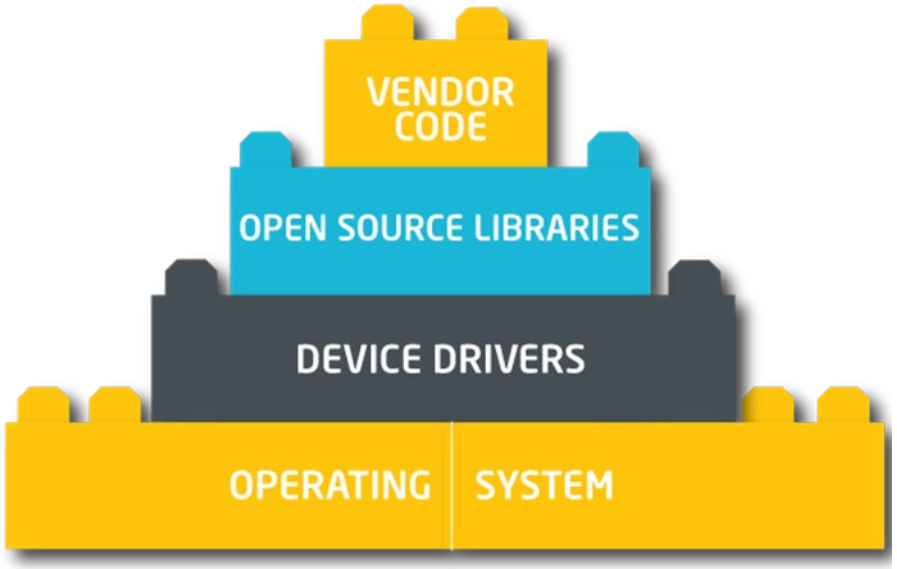
•What is the intended use of the device?

This includes not only where and by whom the device will be used, but also when and how often it will be used. Security controls should be tailored to the end users and to their environments.

•How likely is a cybersecurity breach?

While the likelihood of a cybersecurity breach may be difficult to quantify, manufacturers should consider what knowledge and access would be required to carry out an attack and how valuable the data collected by the device might be to potential hackers

WHAT ARE THE MAIN CHALLENGES ON MARKET BASED ON THE TIC INDUSTRY'S EXPERIENCE?



- Cyber security is a moving target
  - A product with no vulnerabilities today will likely not stay that way forever.
  - What do you do when a component of an IoT device is found to be vulnerable?
- Manufacturers are responsible for ensuring the security of the custom code they develop and must fix vulnerabilities affecting their products lifetime.
- IoT product vendors must have the ability to securely patch the code they develop but must also be able to securely patch the *operating system*, *device drivers* and open *source libraries* the device uses.

TIC SECTOR AND THE CYBER SECURITY OF MEDICAL DEVICES IN NORTH AMERICA:

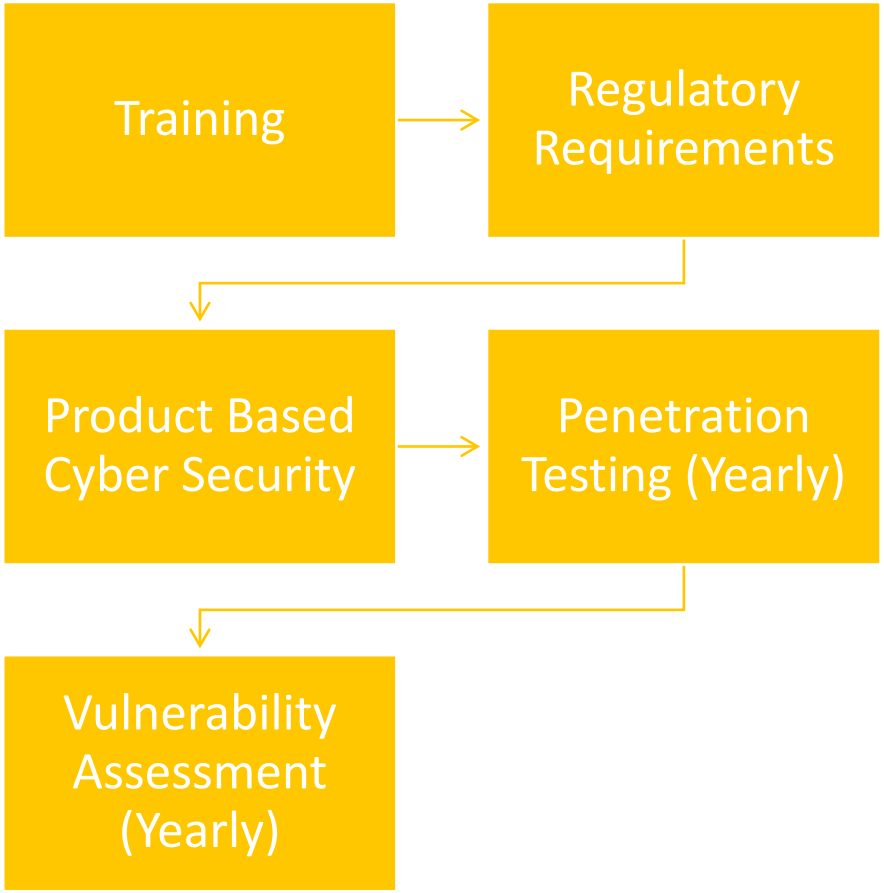
2

WHAT ARE THE BEST PRACTICES MANUFACTURERES SHOULD TAKE INTO CONSIDERATION FOR MITIGATING RISKS AND ENSURING COMPLIANCE WITH CYBER SECURITY REQUIRMENTS IN NORTH AMERICA?

What are the best practices manufacturers should take into consideration for mitigating risks and ensuring compliance with cybersecurity requirements in North America?

- An effective Cyber Security Plan should incorporate both premarket and postmarket phases
- Address risk management from device conception to disposal.
- Software-enabled devices will require a plan for maintaining security throughout the device lifecycle.
- The cybersecurity plan should also include a process for monitoring and managing the ongoing security of the device in the face of emerging vulnerabilities.

What are the best practices manufacturers should take into consideration for mitigating risks and ensuring compliance with cybersecurity requirements in North America?



What are the best practices manufacturers should take into consideration for mitigating risks and ensuring compliance with cybersecurity requirements in North America?

Training Organizational Controls

- Product Design Documentation
- Product Risk
- Risk Controls
- Access-Controls-User Authorization
- Sensitive Date
- Remote Communication
- Product Management
- Software Lifecycle Management

TIC SECTOR AND THE CYBER SECURITY OF MEDICAL DEVICES IN NORTH AMERICA

3

CAN YOU ADDRESS THE NEED FOR VA AND PEN TESTING FOR CERTAIN CATEGORIES OF MEDICAL DEVICES, HOW TO DEAL WITH MEDICAL APPS AND CURRENT CHALLENGES? (HOW ARE THEY DIFF BUT INTERDEPENDENT) ?

CAN YOU ADDRESS THE NEED FOR VA AND PEN TESTING FOR CERTAIN CATEGORIES OF MEDICAL DEVICES, HOW TO DEAL WITH MEDICAL APPS AND CURRENT CHALLENGES? (HOW ARE THEY DIFFERENT BUT INTERDEPENDENT)

"annual basis, Supplier will engage a reputable third party assessor to perform a vulnerability assessment to identify any issues with configuration of firewalls, web services, servers and other system components that could result in access vulnerabilities"

Thank You!!!

George Strom

Director of IOT

Intertek- Connected World

Phone: 617-470-1705

Email: george.strom@intertek.com

Suzanne B. Schwartz, MD, MBA

Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health (CDRH)
U.S. Food and Drug Administration

TIC COUNCIL
Independent Voice of Trust

Michelle Jump

Global Regulatory Advisor
Medical Device Security
MedSec

TIC Sector and the Cybersecurity of Medical Devices in North America

George Strom

Director of IOT
Intertek

Webinar

30th September 2020 - 11:00 - 12:30 (EST)

Roberta Telles

Senior Policy Advisor

TIC Council

rtelles@tic-council.org

Follow us online

@TICCouncil

TIC Council

Wikipedia page:
Testing, inspection and certification

TIC-Council.org