Busting Mythconceptions about the FDA's Refuse-to-Accept Policy for Cybersecurity

PLAUSIBLE

BUSTED

CONFIRMED

Garrett Schumacher
Technical Director of Product Security
Velentium

Medical Device Engineering: Your IP. Designed and Built.

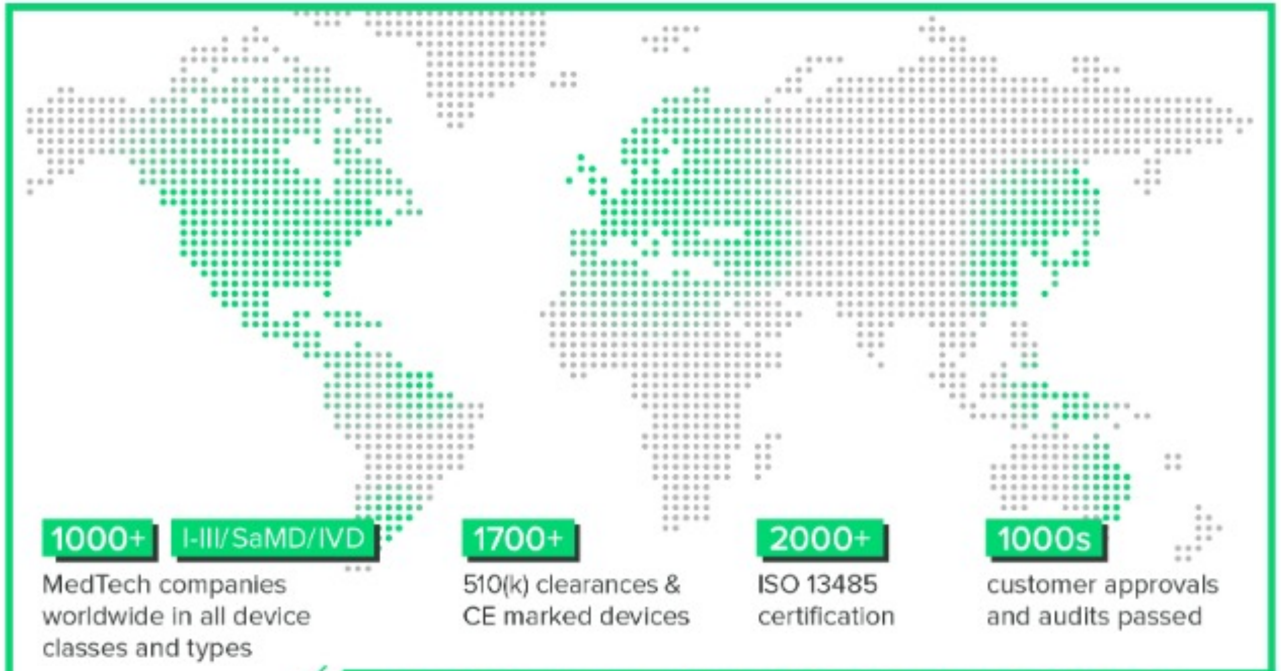
BUILT FOR MEDTECH.
TRUSTED BY MEDTECH.

100+
years industry experience

522k
podcast listeners

200k+
look to us for the latest in quality

#1
blog and podcast in the industry



1000+ **I-III/SaMD/IVD**
MedTech companies worldwide in all device classes and types

1700+
510(k) clearances & CE marked devices

2000+
ISO 13485 certification

1000s
customer approvals and audits passed

TRUSTED BY LEADING MEDTECH COMPANIES GLOBALLY

G2 CROWD
LEADER
MEDICAL QMS SOFTWARE
★★★★☆
Since Spring 2021

G2 CROWD
LEADER
QMS SOFTWARE
★★★★☆
Since Winter 2019

“Best QMS I have ever used…”

This is the easiest eQMS I have used in the 20 years I have been in the Medical Device Industry. ***It is simple, intuitive and easy to use…*** We are successfully implementing a Quality Culture.

- Director of Regulatory Affairs
& Quality Assurance

“Modern QMS Software and Outstanding Customer Service.”

★★★★★

“Demystifying QMS and Regulatory Requirements”

★★★★★

“Makes your QMS Simple and Effective”

★★★★★

greenlight guru

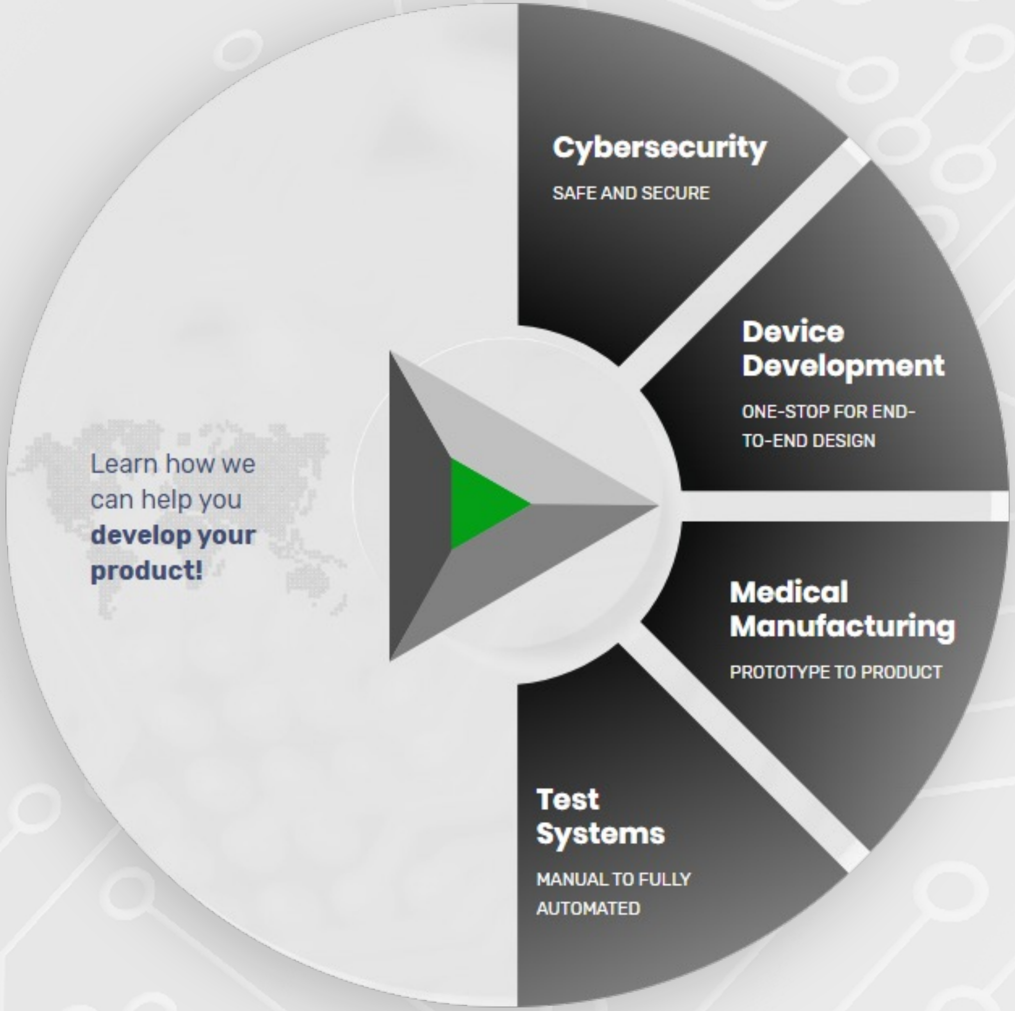
How We Are Different

Cybersecurity

Velentium's depth and breadth of development experience, as well as our ability to navigate the constraints of secure medical device development, makes us an industry leader in device security.

Test Systems

Velentium's Subject Matter Experts can design you a custom test system, ranging from fully manual to fully automatic, and everything in between.



Learn how we can help you **develop your product!**

Cybersecurity
SAFE AND SECURE

Device Development
ONE-STOP FOR END-TO-END DESIGN

Medical Manufacturing
PROTOTYPE TO PRODUCT

Test Systems
MANUAL TO FULLY AUTOMATED

Device Development

We are a one-stop for secure design, development, production, and post-market services. See how we can take your device from IP to commercialized product today!

Medical Manufacturing

Let Velentium meet your manufacturing needs with our ISO 13485-certified lean QMS and our design and development experts within arms' reach at all times.

Medical Device Engineering: Your IP. Designed and Built.

Velentium's Product Security Team

Cybersecurity Consulting Services

- Development Project Assistance
- Product Security Governance
- Post Market Support Services
- Mobile Device Management (MDM) Services
- Embedded Cybersecurity Training
- Custom Consulting Services

Medical Device Engineering: Your IP. Designed and Built.

Velentium's Product Security Team

- Over the last three years, assisted 80 clients with medical device security and FDA/MDR submission content
- ~100 unique medical device projects
  - Deep brain implants
  - Implanted pumps & stimulators
  - AEDs, pacemakers & ventilators
  - Wearable diagnostic devices
  - Mobile, web & cloud
  - SaMD & ML/AI
  - Diagnostic laboratory equipment

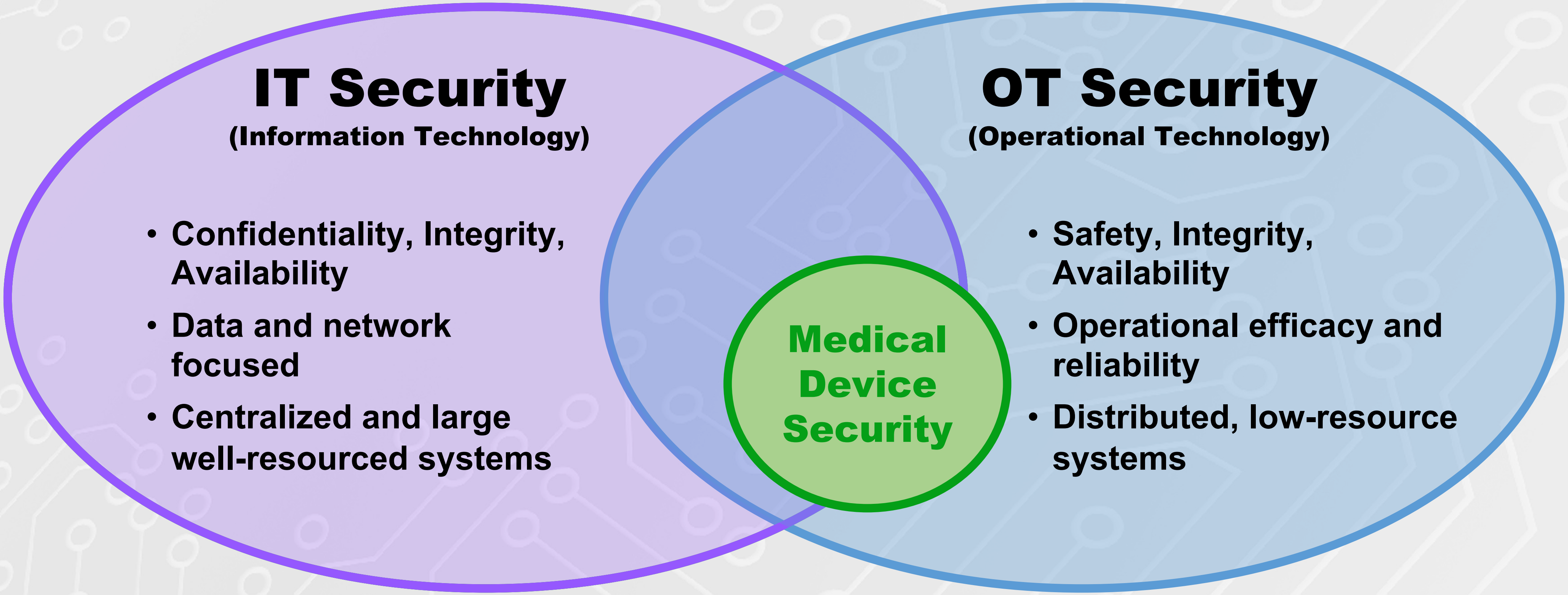
Myth

Cybersecurity is an IT Problem

BUSTED

Medical Device Engineering: Your IP. Designed and Built.

OT Security vs. IT Security



IT Security

(Information Technology)

- Confidentiality, Integrity, Availability
- Data and network focused
- Centralized and large well-resourced systems

OT Security

(Operational Technology)

- Safety, Integrity, Availability
- Operational efficacy and reliability
- Distributed, low-resource systems

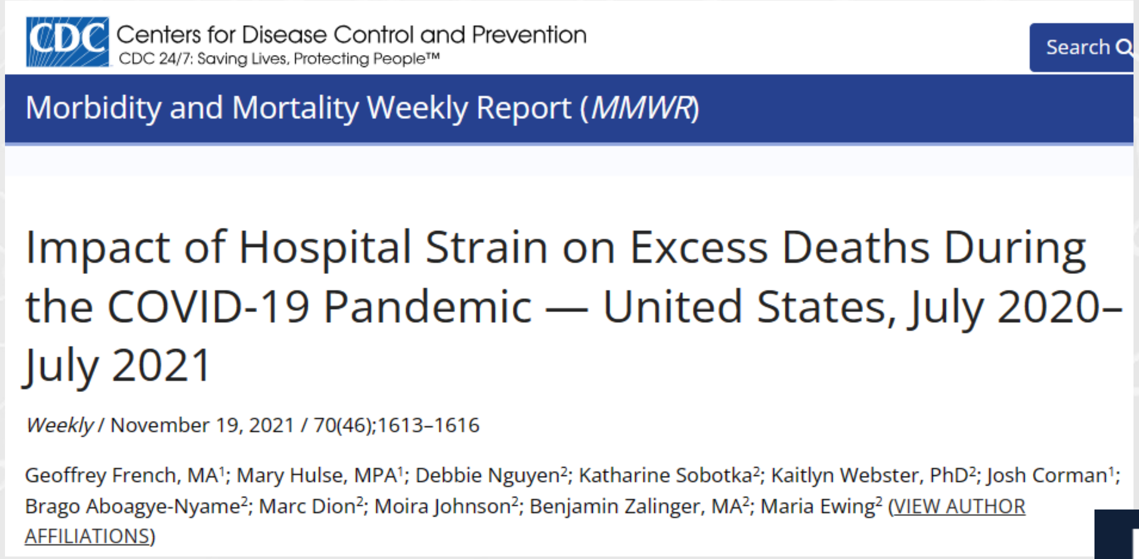
Medical Device Security

Medical Device Engineering: Your IP. Designed and Built.

Myth:

Patients are the Most Important Stakeholder in Medical Cybersecurity

CONFIRMED



CDC Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™

Search

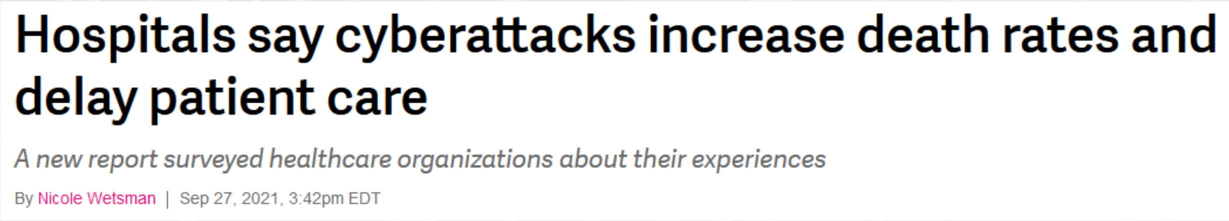
Morbidity and Mortality Weekly Report (*MMWR*)

Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic — United States, July 2020–July 2021

Weekly / November 19, 2021 / 70(46);1613–1616

Geoffrey French, MA[1]; Mary Hulse, MPA[1]; Debbie Nguyen[2]; Katharine Sobotka[2]; Kaitlyn Webster, PhD[2]; Josh Corman[1]; Brago Aboagye-Nyame[2]; Marc Dion[2]; Moira Johnson[2]; Benjamin Zalinger, MA[2]; Maria Ewing[2] (VIEW AUTHOR AFFILIATIONS)

https://www.cdc.gov/mmwr/volumes/70/wr/mm7046a5.htm

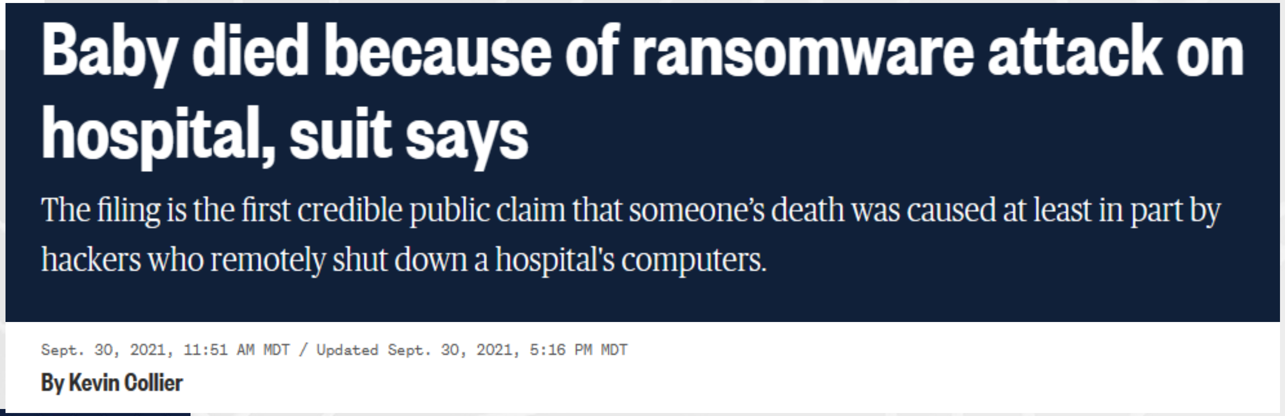


Hospitals say cyberattacks increase death rates and delay patient care

A new report surveyed healthcare organizations about their experiences

By Nicole Wetsman | Sep 27, 2021, 3:42pm EDT

https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients



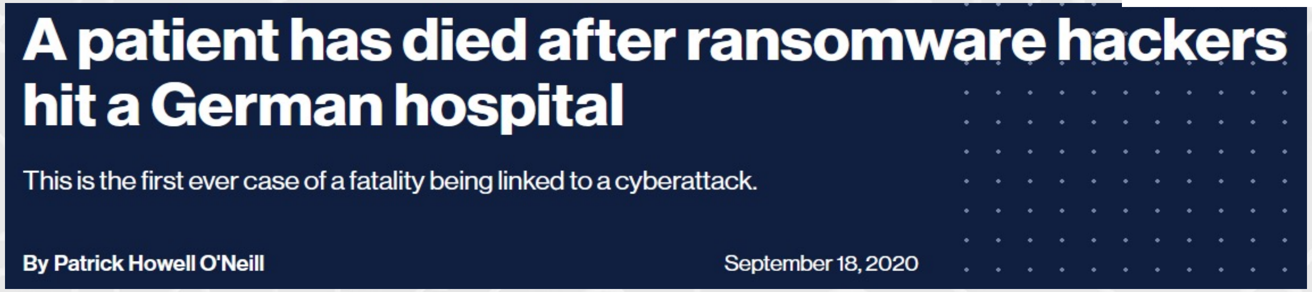
Baby died because of ransomware attack on hospital, suit says

The filing is the first credible public claim that someone's death was caused at least in part by hackers who remotely shut down a hospital's computers.

Sept. 30, 2021, 11:51 AM MDT / Updated Sept. 30, 2021, 5:16 PM MDT

By Kevin Collier

https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465



A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

By Patrick Howell O'Neill September 18, 2020

https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/

Key FDA Terms

- ✓ "**Safety and Efficacy**" – Original FDA medical device mandate
- ✓ "**Reasonable assurance the device and related systems are cybersecure**" – Omnibus / RTA Policy
- ✓ FDA Panel at DEF CON 31 Biohacking Village Talks
  - ○ Be sure to check their YouTube channel for the recordings to be posted
  - ○ https://www.youtube.com/@BiohackingVillage

		“Understanding”	
		Knowns	Unknowns
“Awareness”	Known	Known Knowns	Known Unknowns
	Unknown	Unknown Knowns	Unknown Unknowns

Medical Device Engineering: Your IP. Designed and Built.

		“Understanding”	
		Knowns	Unknowns
“Awareness”	Known	Things we are aware of and understand	Things we are aware of but do not understand
	Unknown	Things we understand but are not aware of	Things we neither understand nor are aware of

		“Understanding”	
		Knowns	Unknowns
“Awareness”	Known	Things we are aware of and understand	Things we are aware of but do not understand
	Unknown	Things we understand but are not aware of	Things we neither understand nor are aware of

Medical Device Engineering: Your IP. Designed and Built.

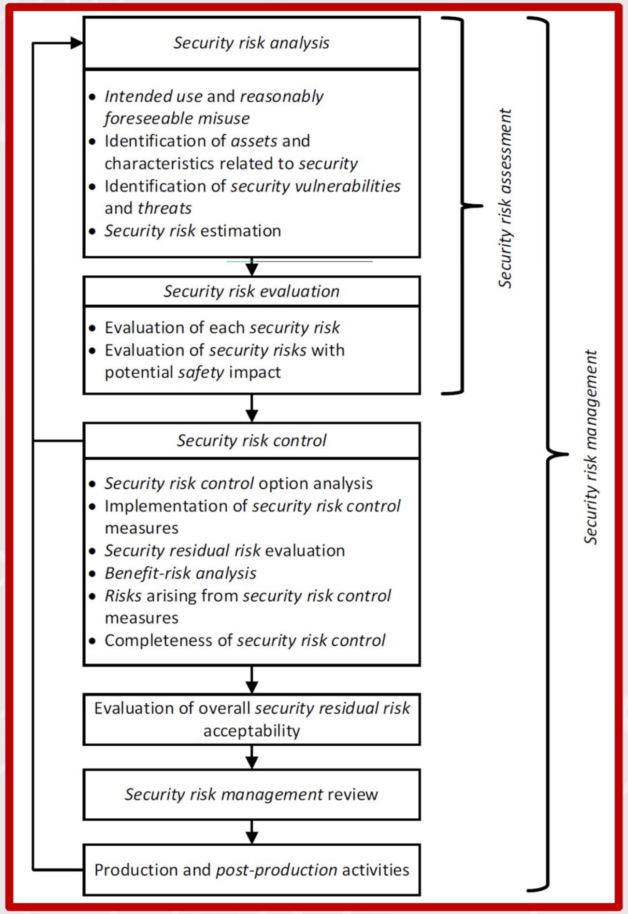
Security Risk Management

1. **Identify potential risks** (awareness)
2. **Analyze and assess risks** (understanding)
3. **Manage risk via:**
   - Accepting it → unreasonable assurance now
   - Reducing it → design and implementation of controls
   - Removing it → making an architectural or design change
   - Transferring it → communication to users, agreements, etc.
4. **Repeat / Maintain**

Various and appropriate ways in which to do this at different stages of the complete product lifecycle

2 Risk Management Paths

- ANSI/AAMI TIR57:2016 (R2023) Principles For Medical Device Security - Risk Management
- ANSI/AAMI SW96:2023 Standard For Medical Device Security - Security Risk Management For Device Manufacturers



Security risk analysis

- *Intended use* and *reasonably foreseeable misuse*
- Identification of *assets* and characteristics related to *security*
- Identification of *security vulnerabilities* and *threats*
- *Security risk* estimation

Security risk evaluation

- Evaluation of each *security risk*
- Evaluation of *security risks* with potential *safety* impact

Security risk control

- *Security risk control* option analysis
- Implementation of *security risk control* measures
- *Security residual risk* evaluation
- *Benefit-risk analysis*
- *Risks* arising from *security risk control* measures
- Completeness of *security risk control*

Evaluation of overall *security residual risk* acceptability

Security risk management review

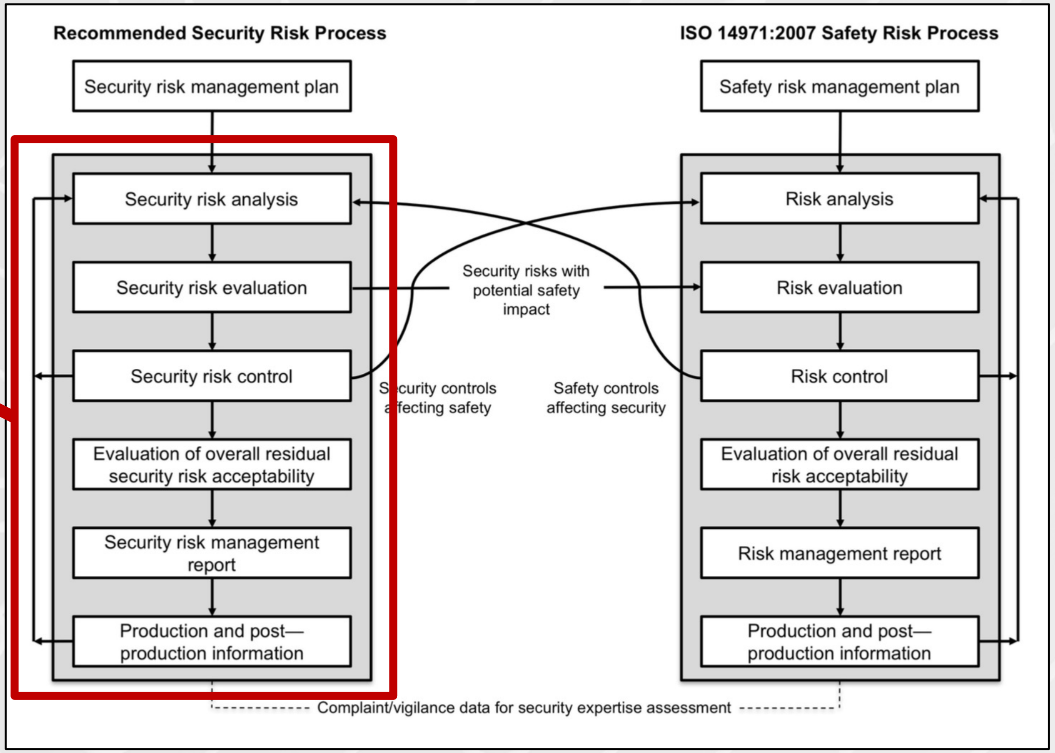
Production and *post-production* activities

Security risk assessment

Security risk management

AAMI SW96:2023

https://array.aami.org/doi/10.2345/9781570208621



Recommended Security Risk Process

Security risk management plan

Security risk analysis

Security risk evaluation

Security risk control

Evaluation of overall residual security risk acceptability

Security risk management report

Production and post—production information

ISO 14971:2007 Safety Risk Process

Safety risk management plan

Risk analysis

Risk evaluation

Risk control

Evaluation of overall residual risk acceptability

Risk management report

Production and post—production information

Security risks with potential safety impact

Security controls affecting safety

Safety controls affecting security

Complaint/vigilance data for security expertise assessment

AAMI TIR57:2016 (R2023)

https://webstore.ansi.org/standards/aami/aamitir572016r2023

Medical Device Engineering: Your IP. Designed and Built.

Myth: Medical Device Security is a New Problem

BUSTED

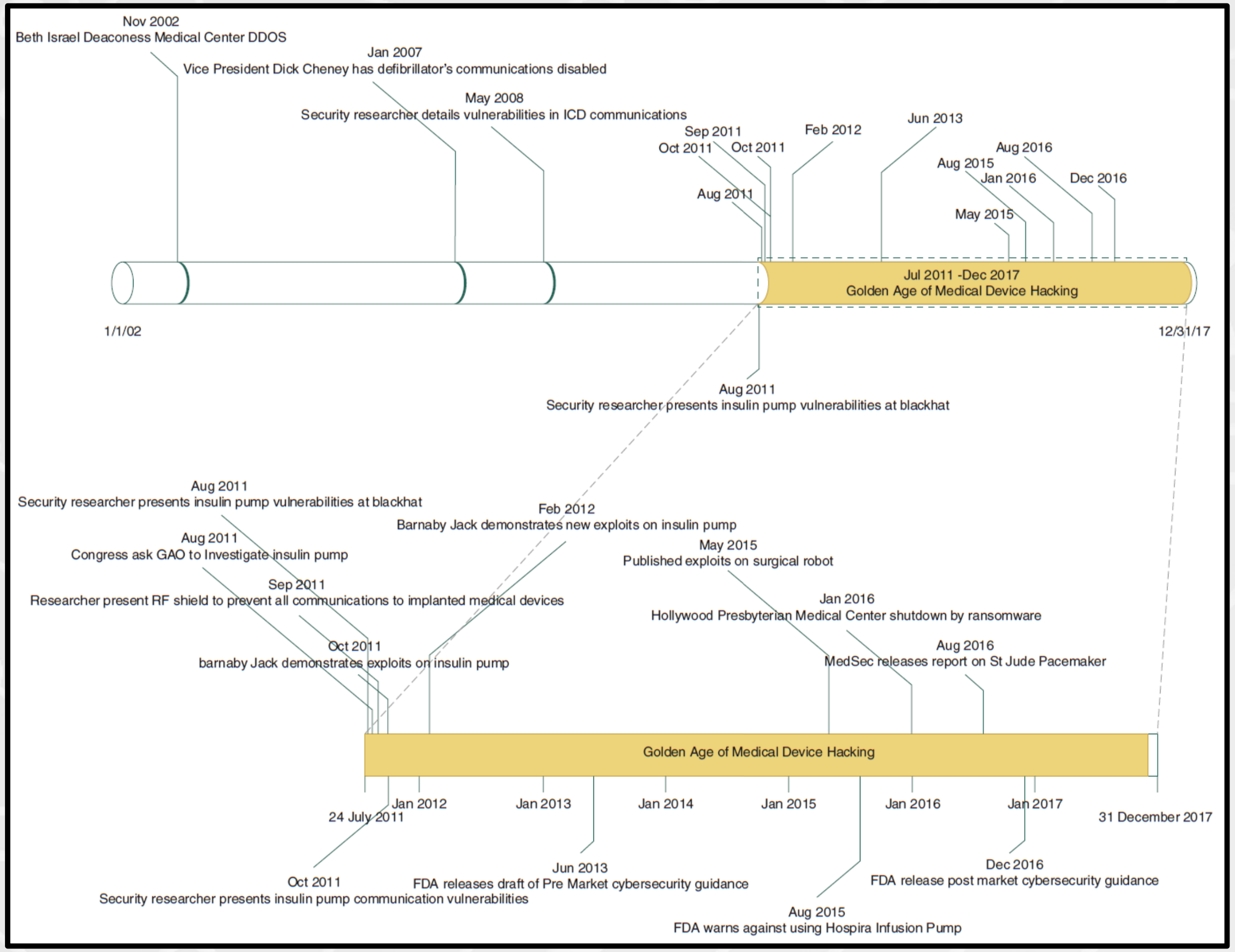
A Brief History: US Market

- **1938** – Federal Food, Drug, and Cosmetic Act (FD&C Act)
- **1970s** – Origins of term ‘Cybersecurity’ and field
- **1976** – FDA Medical Device Amendments to ensure safety and effectiveness of medical devices
- **’90s–’00s** – Additional requirements, such as post-market surveillance and management of devices
- **2005** – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

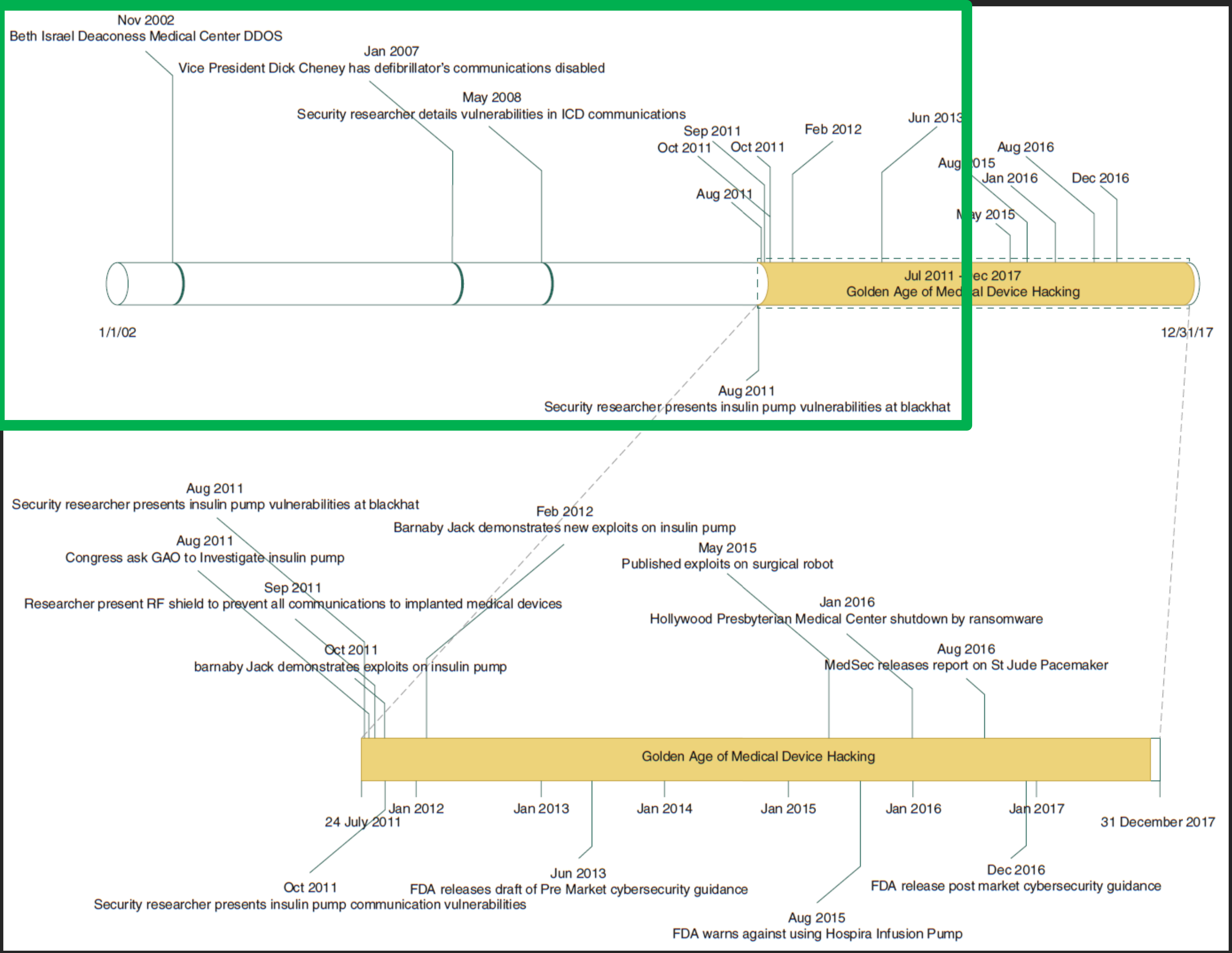
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software

A Brief History

Haider, N., **Gates, C.**, Sengupta, V., & Qian, S. (2019). **Cybersecurity of medical devices: Past, present, and future**. In *Deer's Treatment of Pain* (pp. 811-820). Springer, Cham.



Medical Device Engineering: Your IP. Designed and Built.



Nov 2002
Beth Israel Deaconess Medical Center DDOS

Jan 2007
Vice President Dick Cheney has defibrillator's communications disabled

May 2008
Security researcher details vulnerabilities in ICD communications

Sep 2011

Oct 2011

Oct 2011

Feb 2012

Jun 2013

Aug 2011

Aug 2015

Aug 2016

Jan 2016

Dec 2016

May 2015

Jul 2011 - Dec 2017
Golden Age of Medical Device Hacking

1/1/02

12/31/17

Aug 2011
Security researcher presents insulin pump vulnerabilities at blackhat

Aug 2011
Security researcher presents insulin pump vulnerabilities at blackhat

Feb 2012
Barnaby Jack demonstrates new exploits on insulin pump

Aug 2011
Congress ask GAO to Investigate insulin pump

May 2015
Published exploits on surgical robot

Sep 2011
Researcher present RF shield to prevent all communications to implanted medical devices

Jan 2016
Hollywood Presbyterian Medical Center shutdown by ransomware

Oct 2011
barnaby Jack demonstrates exploits on insulin pump

Aug 2016
MedSec releases report on St Jude Pacemaker

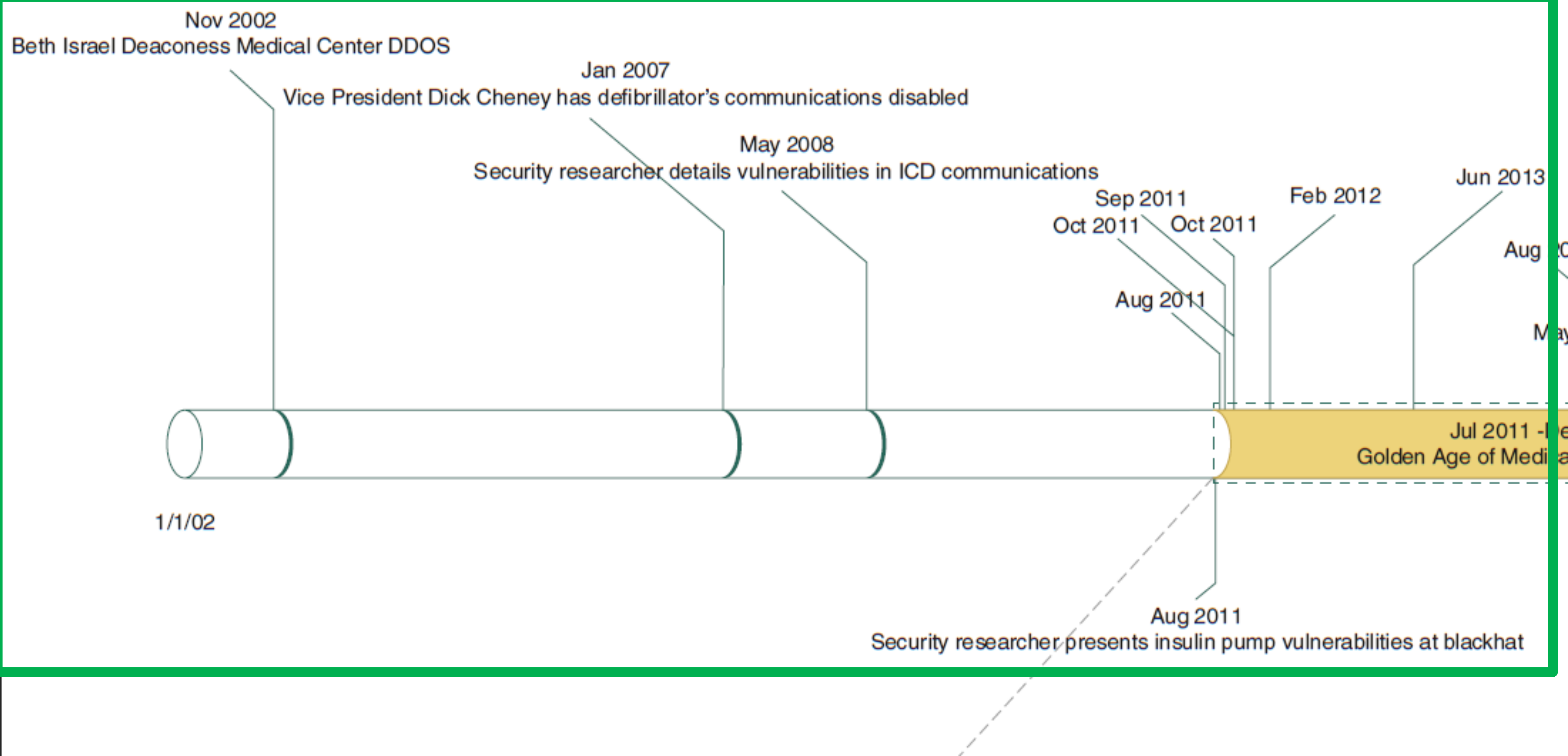
Golden Age of Medical Device Hacking

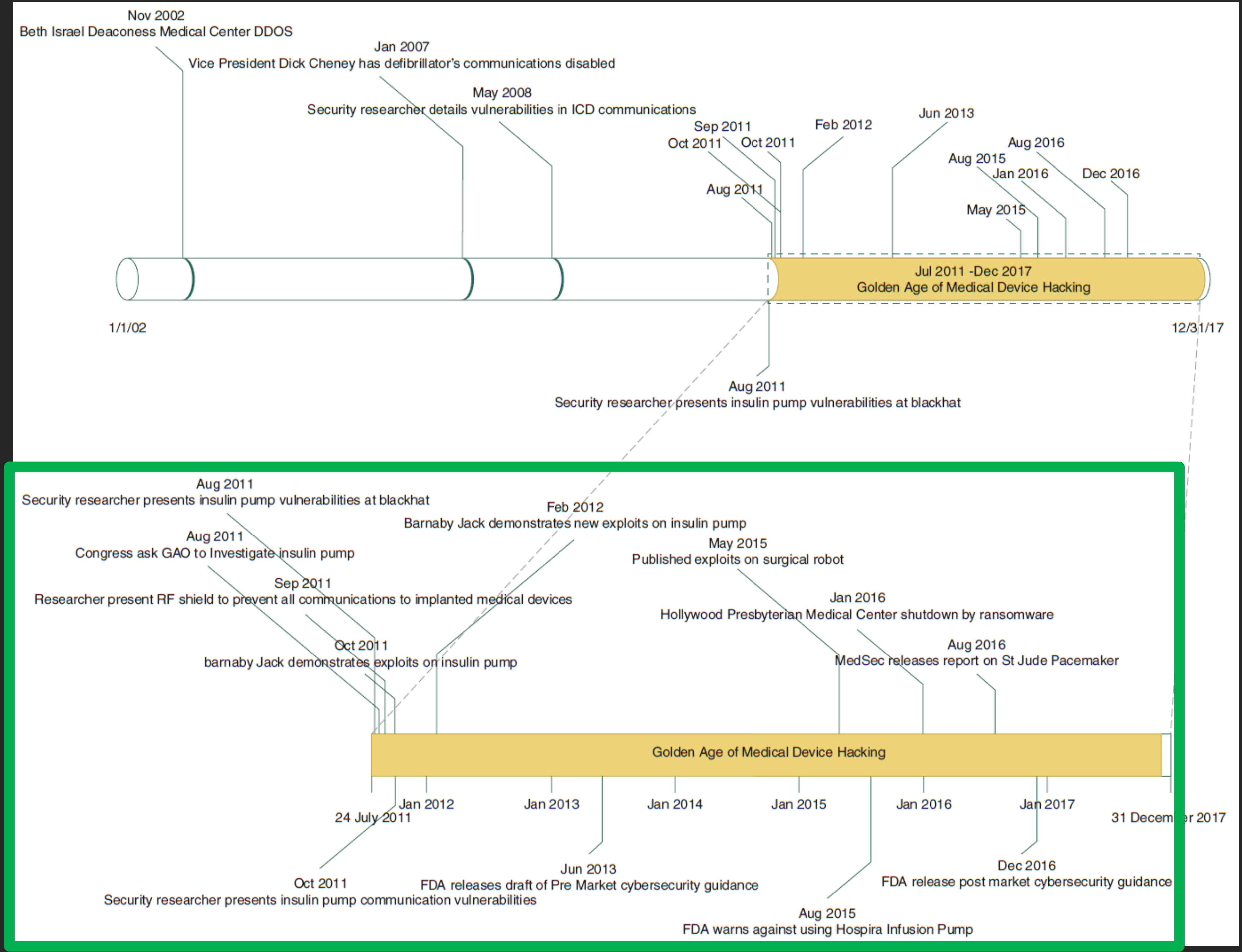
Jun 2013
FDA releases draft of Pre Market cybersecurity guidance

Dec 2016
FDA release post market cybersecurity guidance

Oct 2011
Security researcher presents insulin pump communication vulnerabilities

Aug 2015
FDA warns against using Hospira Infusion Pump


Nov 2002
Beth Israel Deaconess Medical Center DDOS
Jan 2007
Vice President Dick Cheney has defibrillator's communications disabled
May 2008
Security researcher details vulnerabilities in ICD communications
Sep 2011
Oct 2011
Oct 2011
Feb 2012
Jun 2013
Aug 20
Aug 2011
Ma
Jul 2011 -
Golden Age of Medi
1/1/02
Aug 2011
Security researcher presents insulin pump vulnerabilities at blackhat



Nov 2002
Beth Israel Deaconess Medical Center DDOS

Jan 2007
Vice President Dick Cheney has defibrillator's communications disabled

May 2008
Security researcher details vulnerabilities in ICD communications

Sep 2011
Oct 2011
Oct 2011
Aug 2011
Feb 2012
Jun 2013
Aug 2015
Aug 2016
Jan 2016
Dec 2016
May 2015

Jul 2011 -Dec 2017
Golden Age of Medical Device Hacking

1/1/02

12/31/17

Aug 2011
Security researcher presents insulin pump vulnerabilities at blackhat

Aug 2011
Security researcher presents insulin pump vulnerabilities at blackhat

Feb 2012
Barnaby Jack demonstrates new exploits on insulin pump

Aug 2011
Congress ask GAO to Investigate insulin pump

May 2015
Published exploits on surgical robot

Sep 2011
Researcher present RF shield to prevent all communications to implanted medical devices

Jan 2016
Hollywood Presbyterian Medical Center shutdown by ransomware

Oct 2011
barnaby Jack demonstrates exploits on insulin pump

Aug 2016
MedSec releases report on St Jude Pacemaker

Golden Age of Medical Device Hacking

Jan 2012
Jan 2013
Jan 2014
Jan 2015
Jan 2016
Jan 2017

24 July 2011

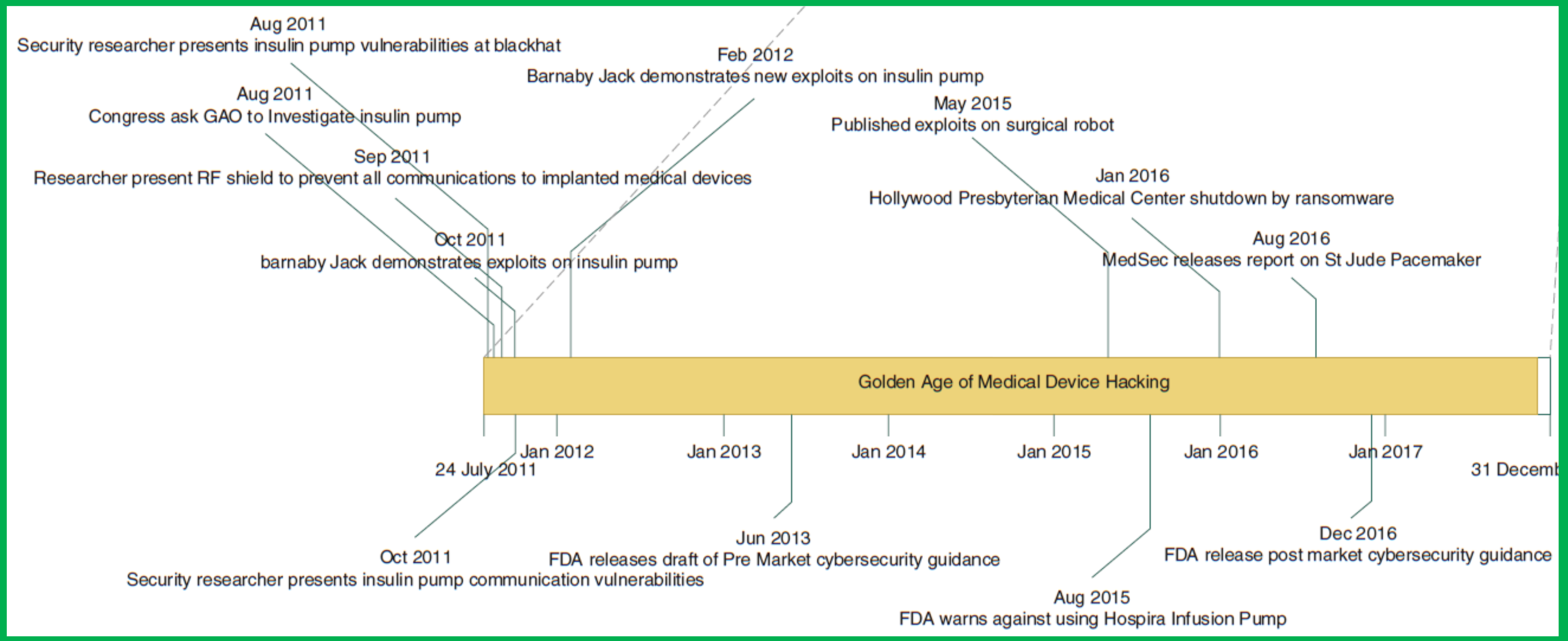
31 December 2017

Jun 2013
FDA releases draft of Pre Market cybersecurity guidance

Dec 2016
FDA release post market cybersecurity guidance

Oct 2011
Security researcher presents insulin pump communication vulnerabilities

Aug 2015
FDA warns against using Hospira Infusion Pump



Aug 2011
Security researcher presents insulin pump vulnerabilities at blackhat

Aug 2011
Congress ask GAO to Investigate insulin pump

Sep 2011
Researcher present RF shield to prevent all communications to implanted medical devices

Oct 2011
barnaby Jack demonstrates exploits on insulin pump

Feb 2012
Barnaby Jack demonstrates new exploits on insulin pump

May 2015
Published exploits on surgical robot

Jan 2016
Hollywood Presbyterian Medical Center shutdown by ransomware

Aug 2016
MedSec releases report on St Jude Pacemaker

Oct 2011
Security researcher presents insulin pump communication vulnerabilities

Jun 2013
FDA releases draft of Pre Market cybersecurity guidance

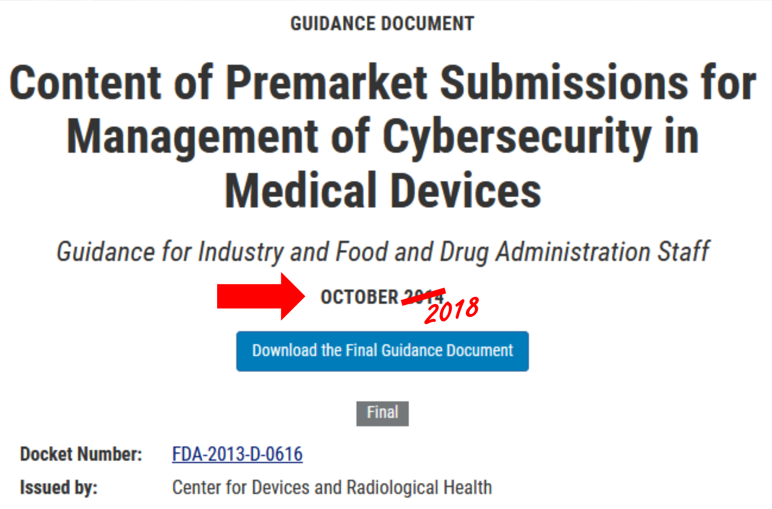
Aug 2015
FDA warns against using Hospira Infusion Pump

Dec 2016
FDA release post market cybersecurity guidance

A Brief History: US Market

- **2014** – FDA added security to submissions
- **2016** – FDA requires MDMs to monitor and maintain fielded devices
- ~~**2018** – Updated premarket guidance~~…

JK ☺



GUIDANCE DOCUMENT

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

OCTOBER ~~2014~~ 2018

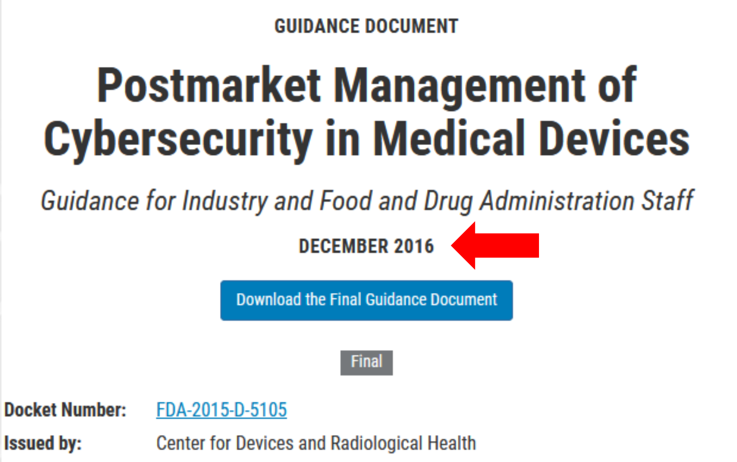
Download the Final Guidance Document

Final

Docket Number: FDA-2013-D-0616

Issued by: Center for Devices and Radiological Health

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices



GUIDANCE DOCUMENT

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

DECEMBER 2016

Download the Final Guidance Document

Final

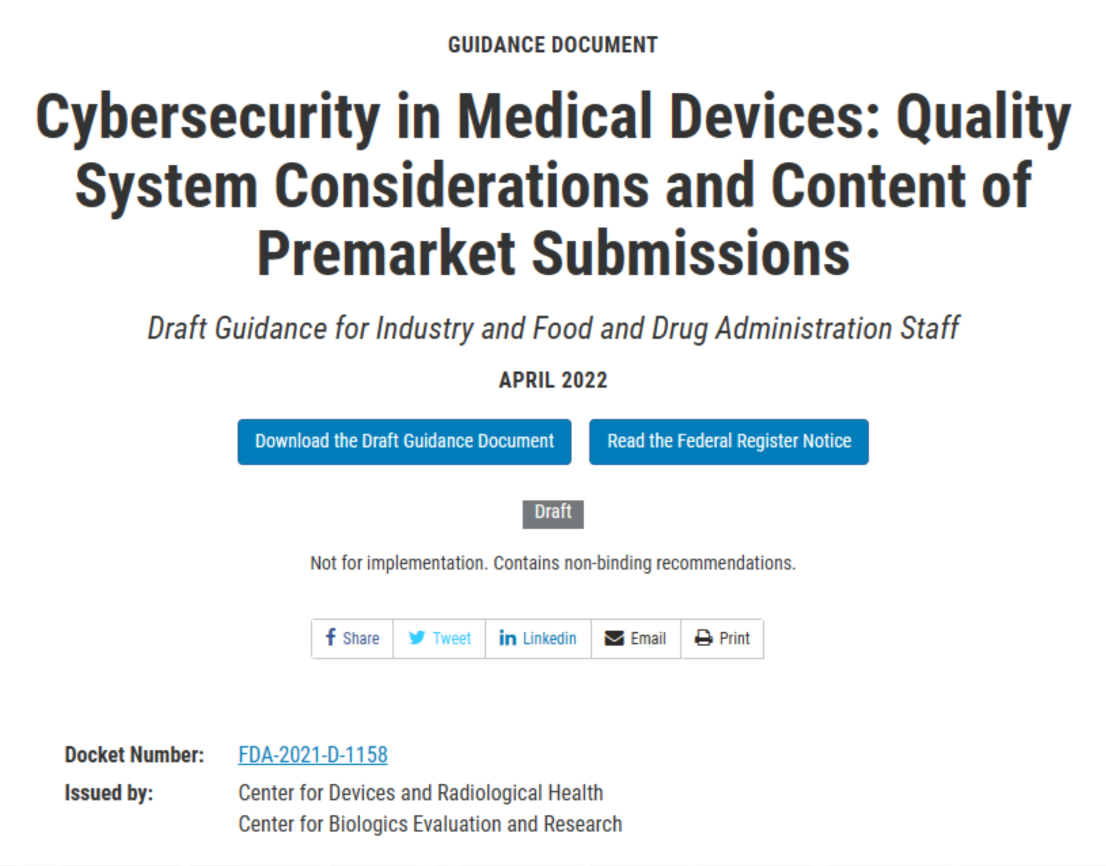
Docket Number: FDA-2015-D-5105

Issued by: Center for Devices and Radiological Health

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

A Brief History: US Market

- **April 2022** – FDA releases draft update to premarket guidance



GUIDANCE DOCUMENT

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Draft Guidance for Industry and Food and Drug Administration Staff

APRIL 2022

Download the Draft Guidance Document
Read the Federal Register Notice
Draft

Not for implementation. Contains non-binding recommendations.

Share
Tweet
Linkedin
Email
Print

Docket Number:	FDA-2021-D-1158
Issued by:	Center for Devices and Radiological Health Center for Biologics Evaluation and Research

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

Content Comparison: 2014 vs 2022

2014 Premarket Guidance

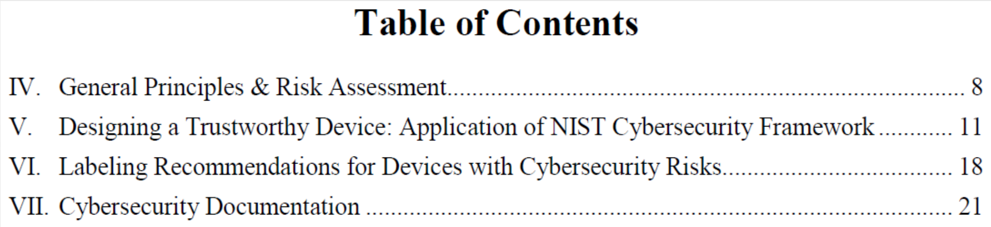
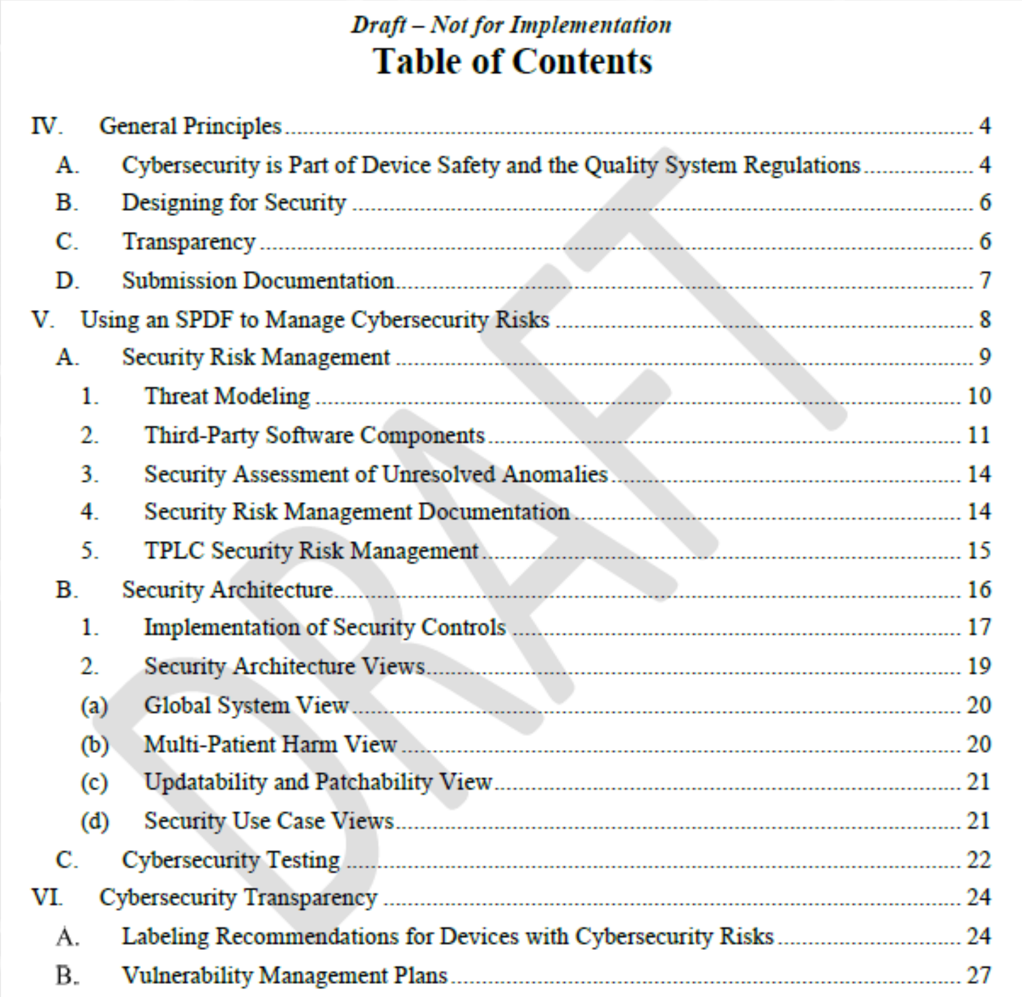


Table of Contents

2022 Draft Premarket Guidance

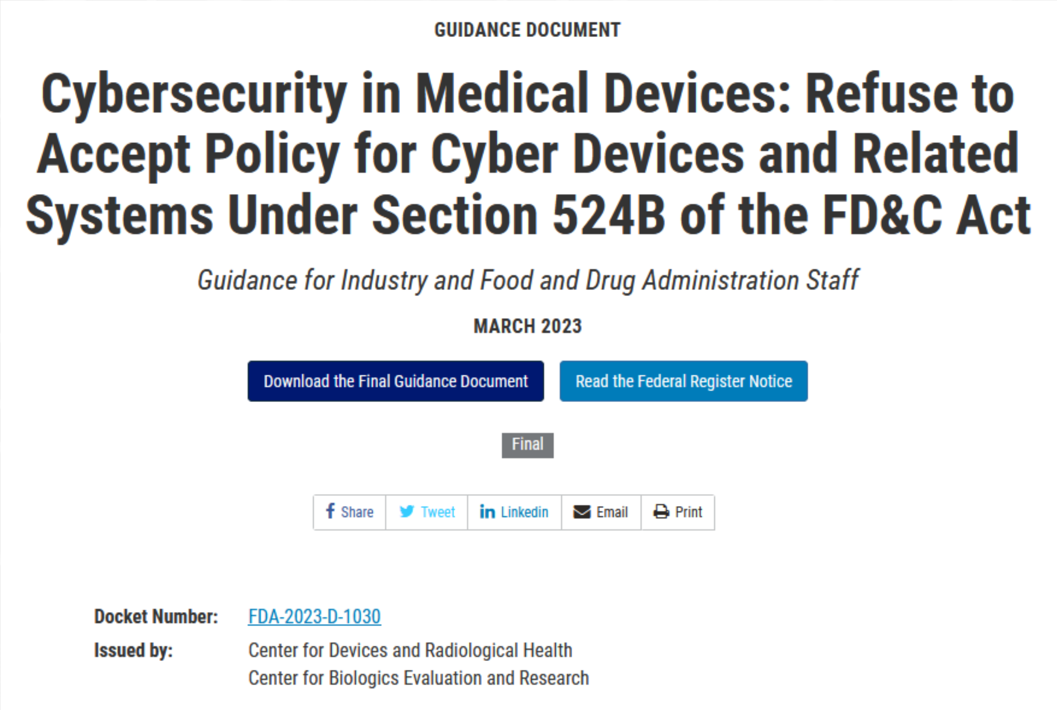


Draft – Not for Implementation

Table of Contents

Modern FDA Requirements

- **December 2022** – "Omnibus bill" (Consolidated Appropriations Act, 2023) signed into law
- Adds Section 524B to FD&C Act



GUIDANCE DOCUMENT

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act

Guidance for Industry and Food and Drug Administration Staff

MARCH 2023

Download the Final Guidance Document
Read the Federal Register Notice
Final
Share
Tweet
Linkedin
Email
Print

Docket Number: FDA-2023-D-1030

Issued by: Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

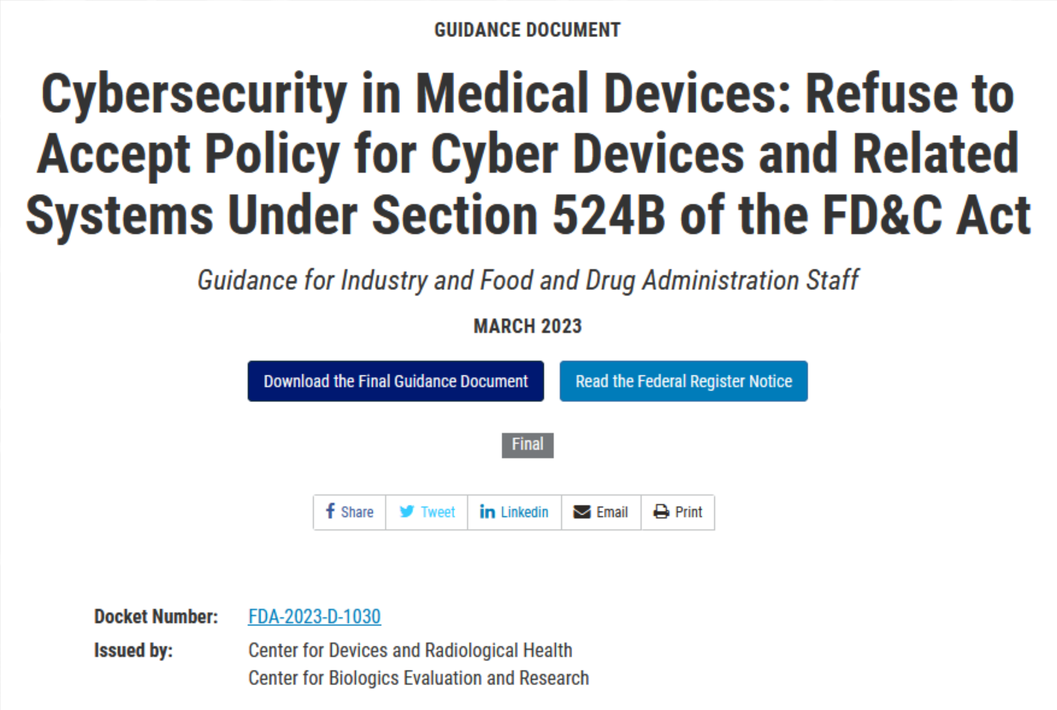
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section

Medical Device Engineering: Your IP. Designed and Built.

Modern FDA Requirements

- **March 2023** – Omnibus bill became effective

“FDA generally intends not to issue ‘refuse to accept’ decisions for premarket submissions… based solely on information required by section 524B of the FD&C Act before October 1, 2023.”



GUIDANCE DOCUMENT

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act

Guidance for Industry and Food and Drug Administration Staff

MARCH 2023

Download the Final Guidance Document
Read the Federal Register Notice
Final
Share
Tweet
Linkedin
Email
Print

Docket Number: FDA-2023-D-1030

Issued by: Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section

VELENTIUM

greenlight guru

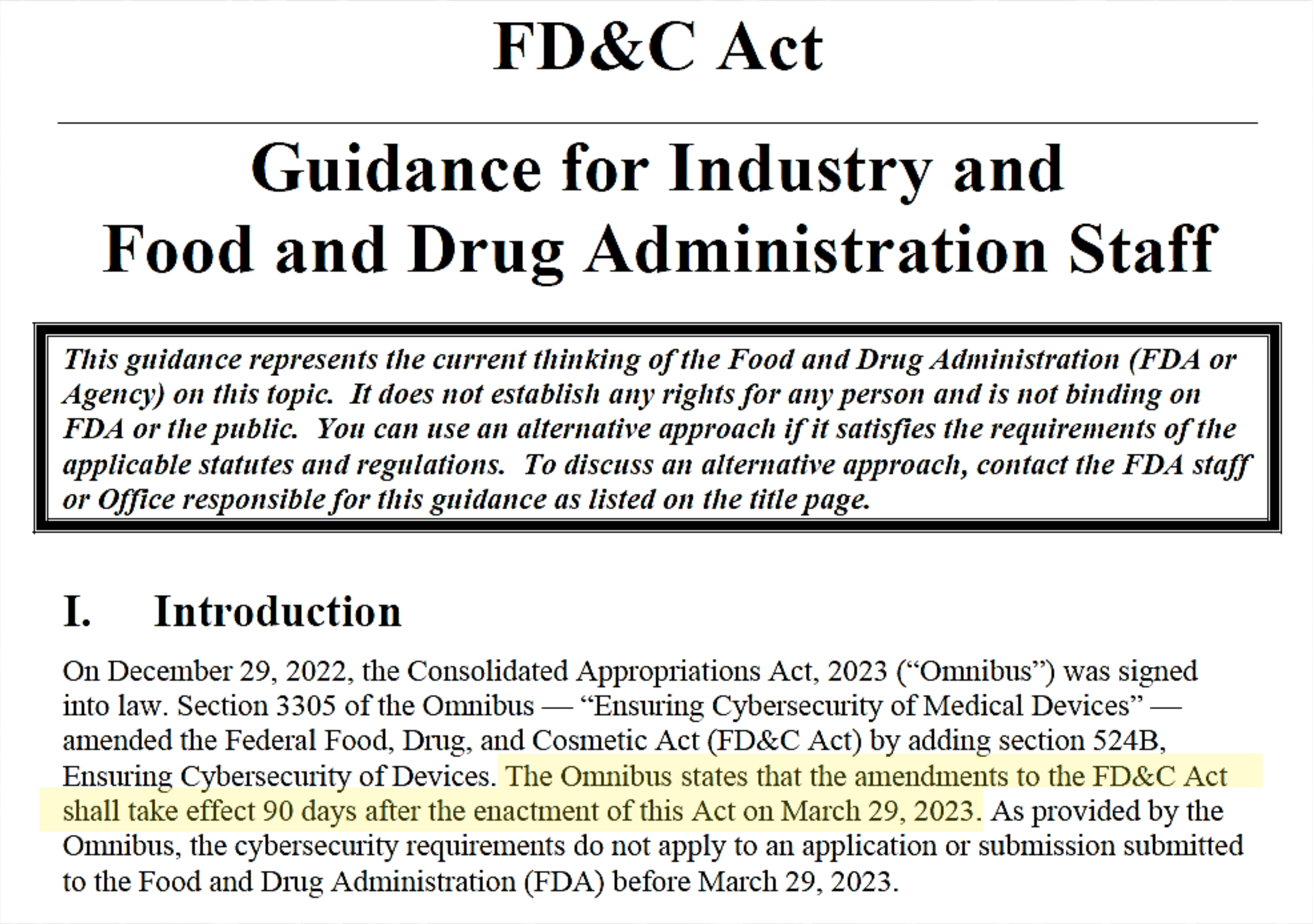
Medical Device Engineering: Your IP. Designed and Built.

Myth:

The FDA's new authority and requirements go into effect October 1, 2023

BUSTED

Medical Device Engineering: Your IP. Designed and Built.



FD&C Act

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

I. Introduction

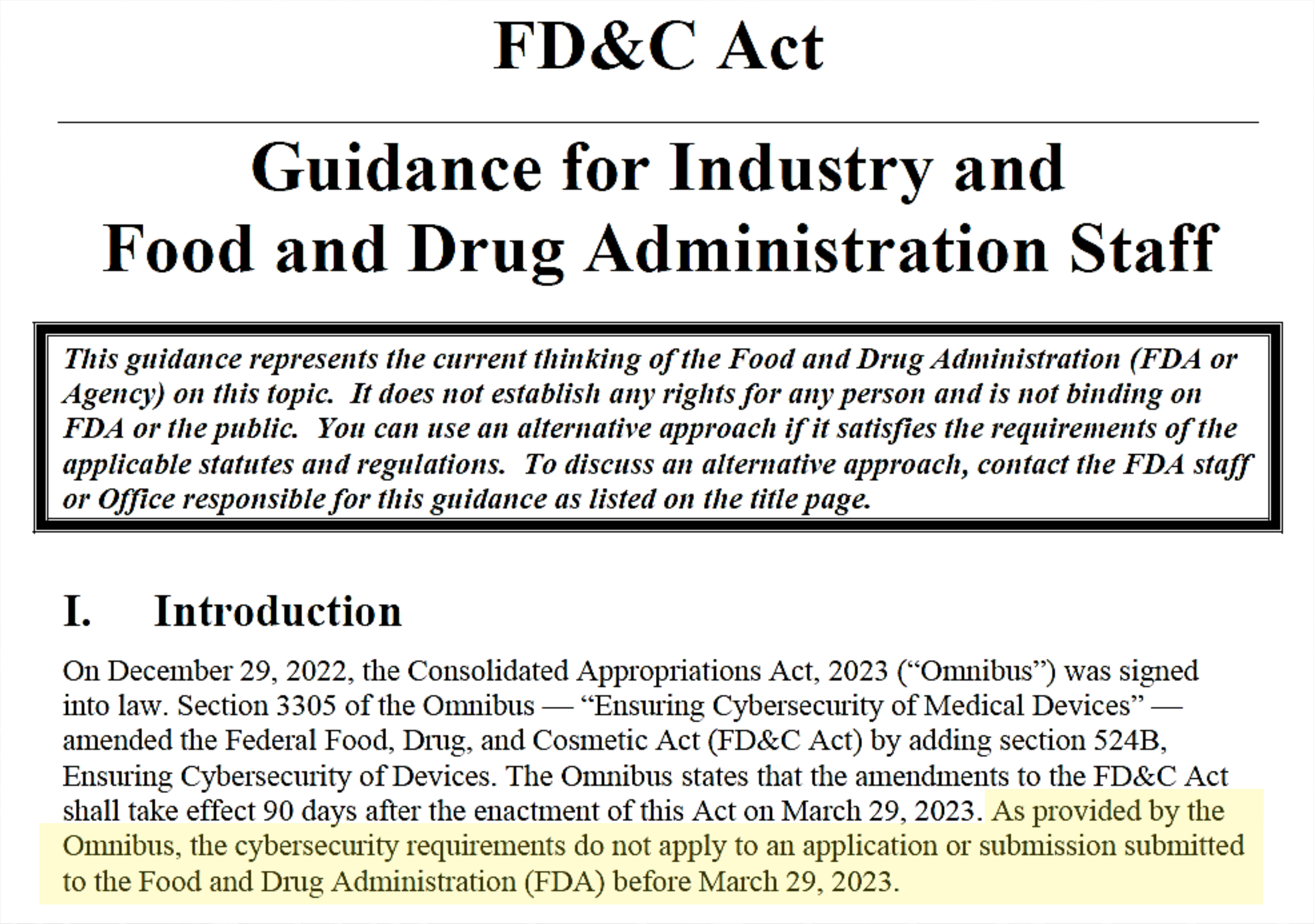
On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus — "Ensuring Cybersecurity of Medical Devices" — amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices. The Omnibus states that the amendments to the FD&C Act shall take effect 90 days after the enactment of this Act on March 29, 2023. As provided by the Omnibus, the cybersecurity requirements do not apply to an application or submission submitted to the Food and Drug Administration (FDA) before March 29, 2023.

Myth:

Legacy devices or devices already approved are not subject to the new FDA requirements

CONFIRMED

Medical Device Engineering: Your IP. Designed and Built.



FD&C Act

Guidance for Industry and Food and Drug Administration Staff

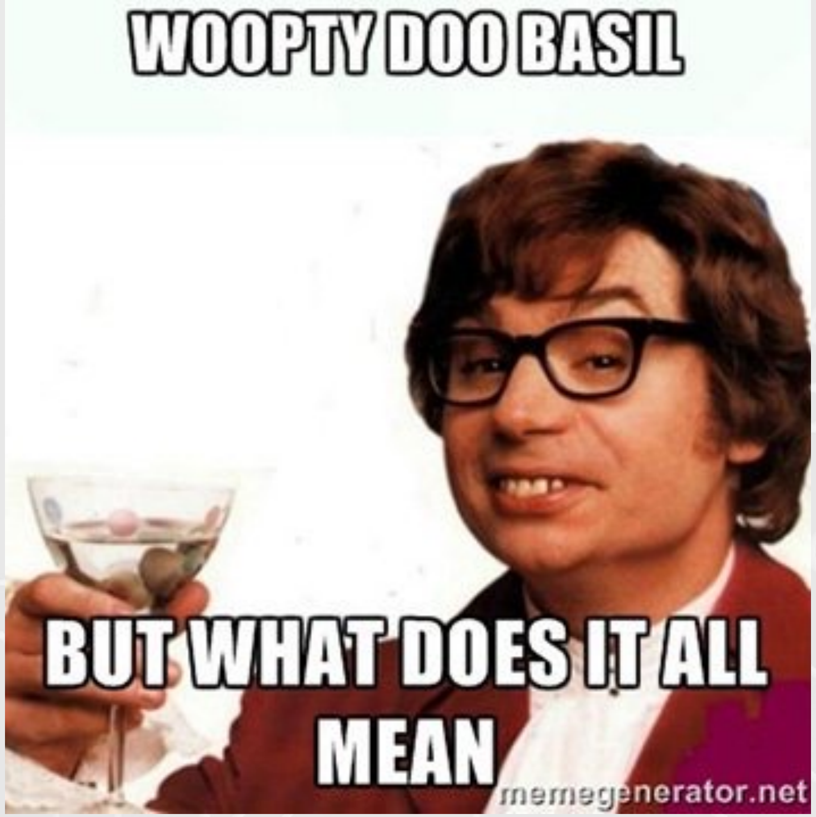
This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

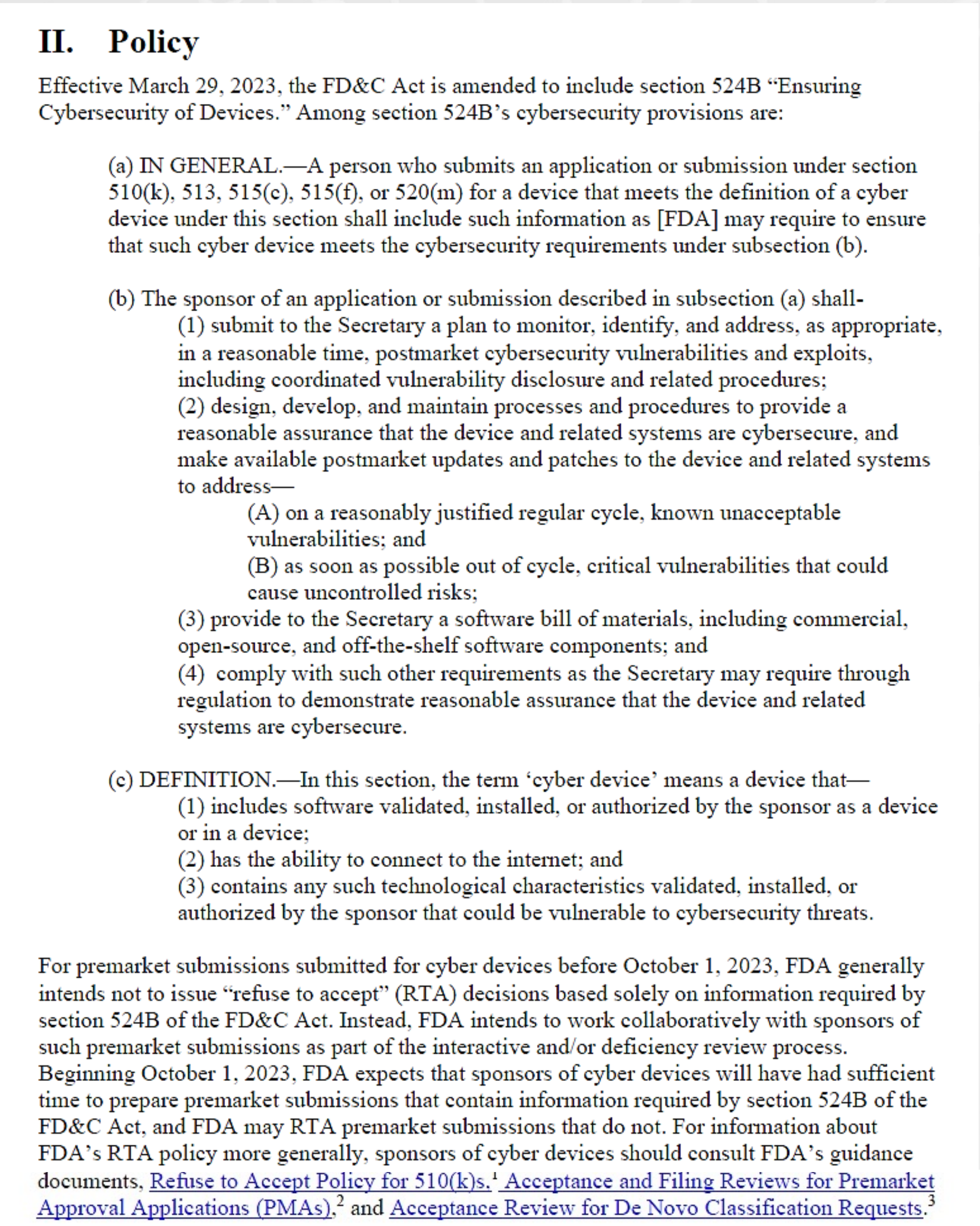
I. Introduction

On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law. Section 3305 of the Omnibus — "Ensuring Cybersecurity of Medical Devices" — amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices. The Omnibus states that the amendments to the FD&C Act shall take effect 90 days after the enactment of this Act on March 29, 2023. As provided by the Omnibus, the cybersecurity requirements do not apply to an application or submission submitted to the Food and Drug Administration (FDA) before March 29, 2023.

Medical Device Engineering: Your IP. Designed and Built.

Modern FDA Requirements





II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

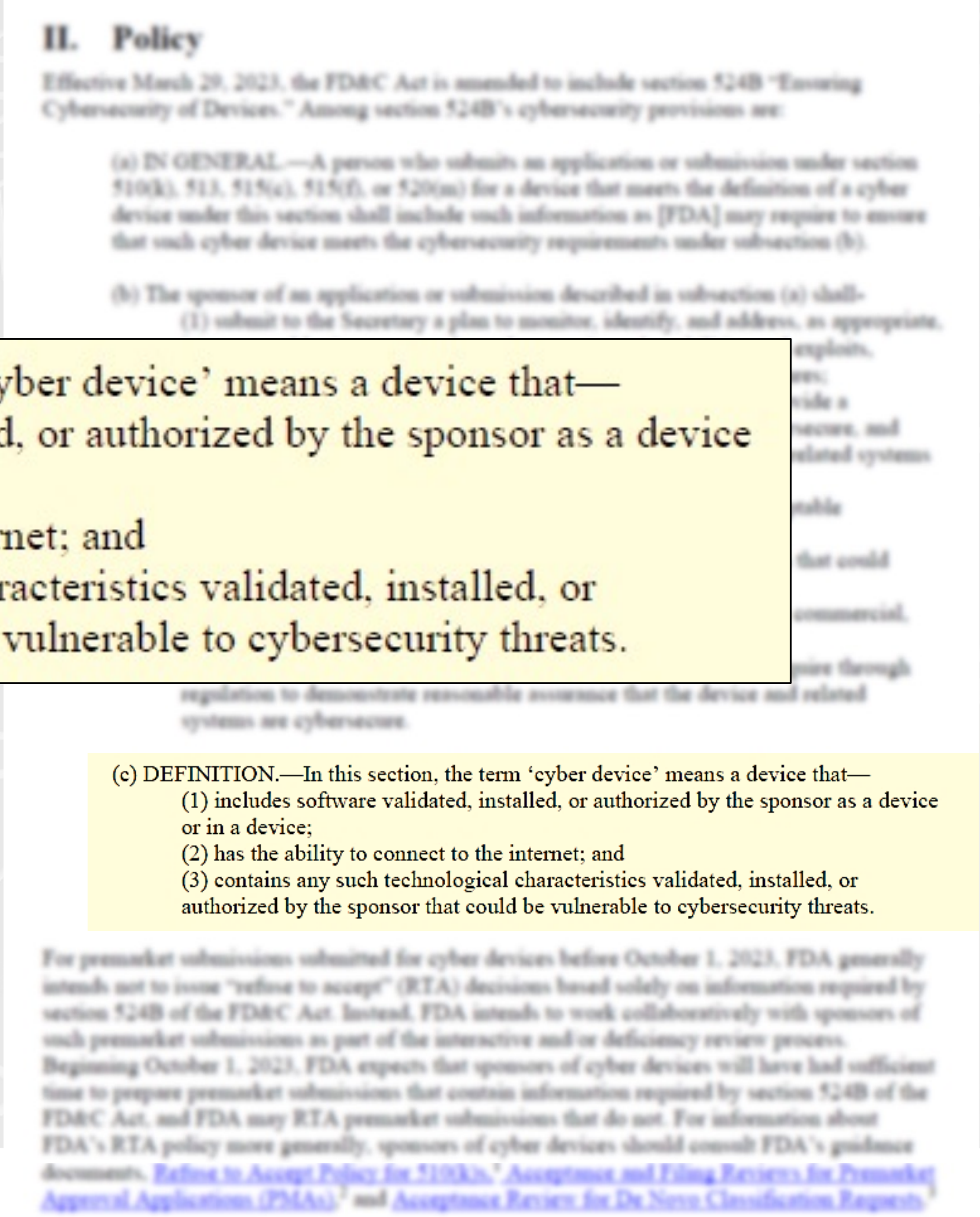
> (a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).
>
> (b) The sponsor of an application or submission described in subsection (a) shall-
> (1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;
> (2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address—
> (A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and
> (B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;
> (3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and
> (4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.
>
> (c) DEFINITION.—In this section, the term 'cyber device' means a device that—
> (1) includes software validated, installed, or authorized by the sponsor as a device or in a device;
> (2) has the ability to connect to the internet; and
> (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s.[1] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[2] and Acceptance Review for De Novo Classification Requests.[3]

Modern FDA Requirements

(c) DEFINITION.—In this section, the term ‘cyber device’ means a device that—
(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;
(2) has the ability to connect to the internet; and
(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

- ✓ Must prove that a device does not have cyber risks as opposed to justifying or claiming it does not



II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-
(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate,
exploits,
res;
vide a
secure, and
elated systems
table
that could
commercial,
uire through
regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

(c) DEFINITION.—In this section, the term ‘cyber device’ means a device that—
(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;
(2) has the ability to connect to the internet; and
(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s, Acceptance and Filing Reviews for Premarket Approval Applications (PMAs), and Acceptance Review for De Novo Classification Requests.

Myth:

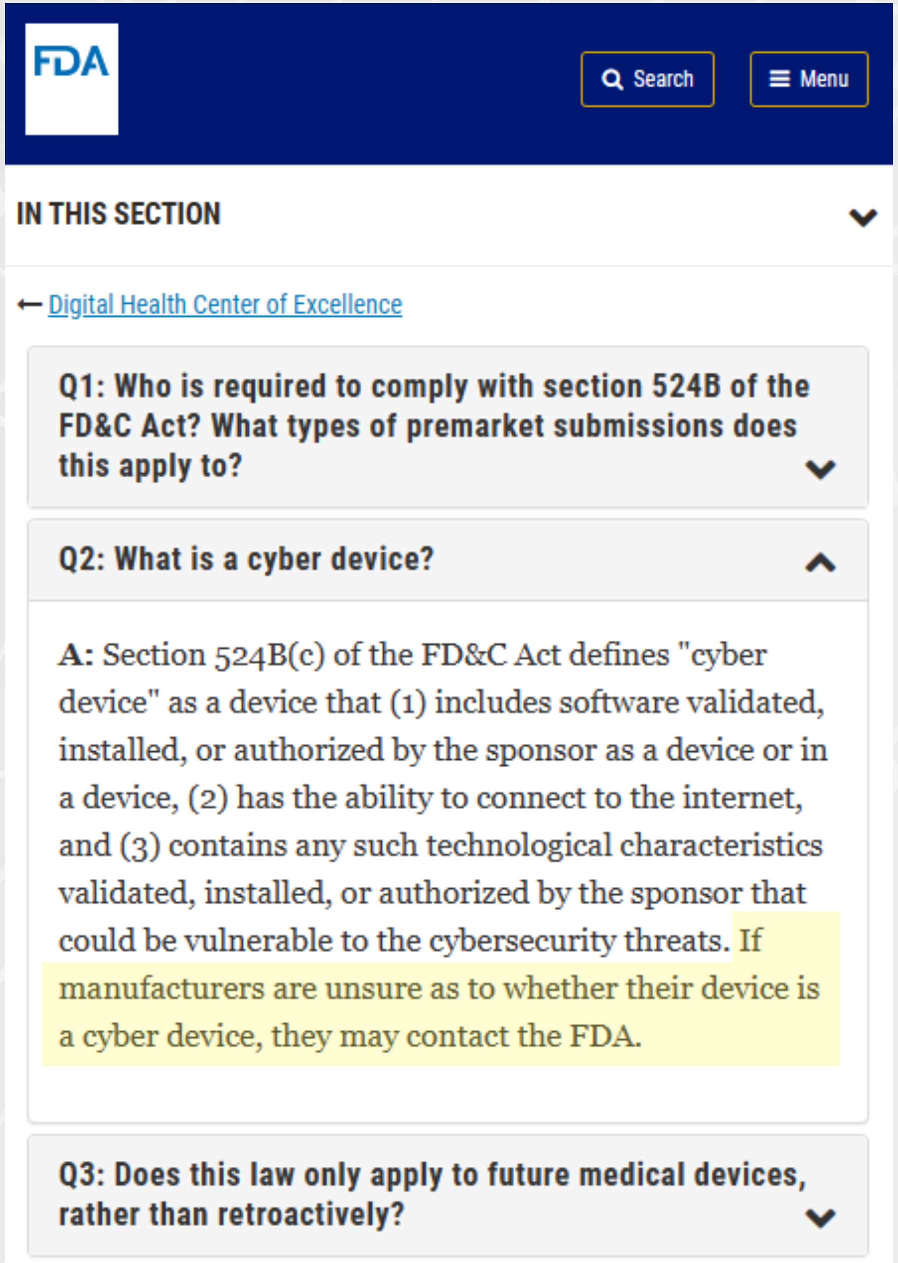
Medical devices that do not connect to the Internet do not apply

PLAUSIBLE

Medical Device Engineering: Your IP. Designed and Built.

What is a cyber device?

- Still a vague description
- Must perform risk assessments to truly know if a device is or is not a *cyber device*
- Can ask FDA directly regarding your device



Q1: Who is required to comply with section 524B of the FD&C Act? What types of premarket submissions does this apply to?

Q2: What is a cyber device?

A: Section 524B(c) of the FD&C Act defines "cyber device" as a device that (1) includes software validated, installed, or authorized by the sponsor as a device or in a device, (2) has the ability to connect to the internet, and (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to the cybersecurity threats. If manufacturers are unsure as to whether their device is a cyber device, they may contact the FDA.

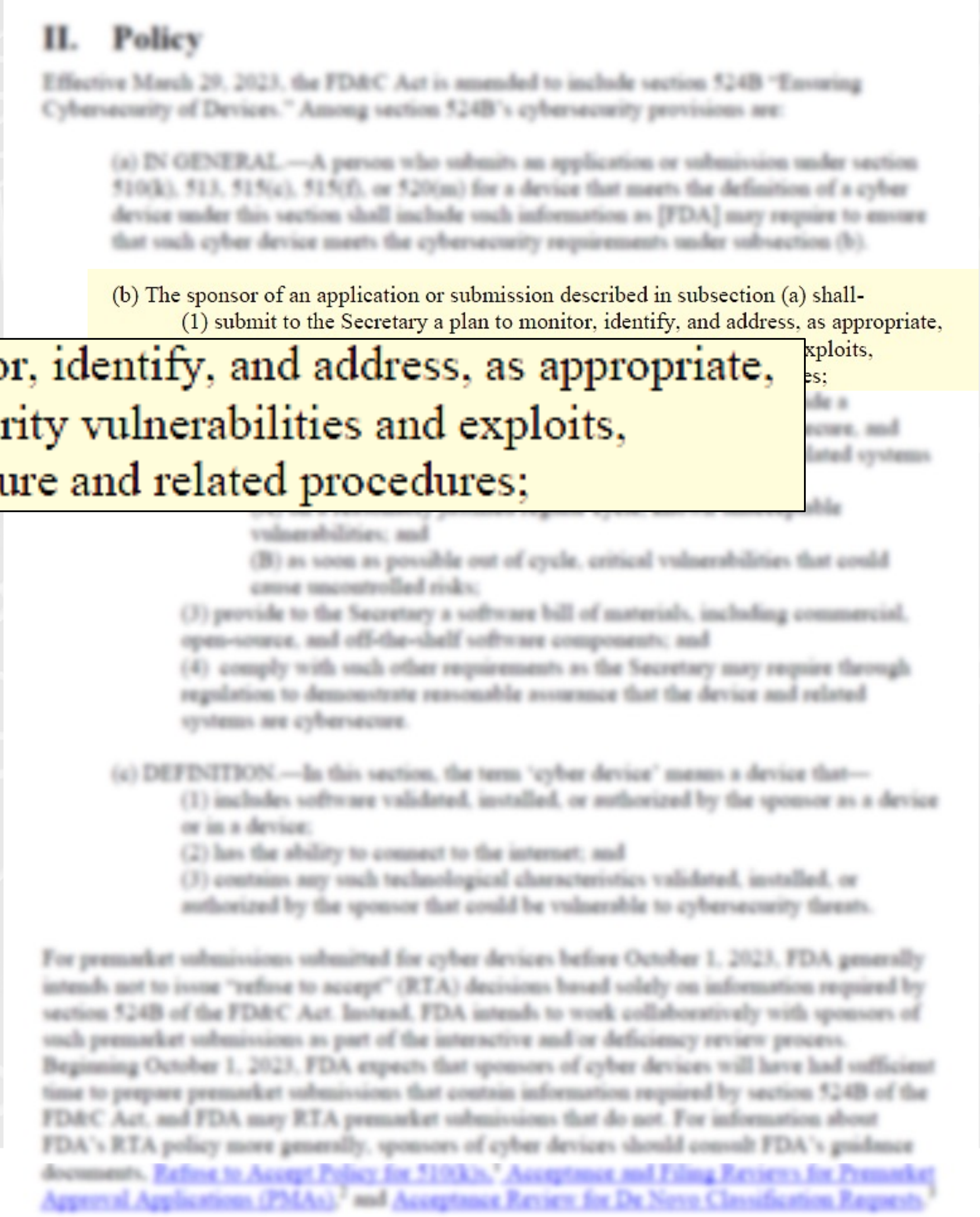
Q3: Does this law only apply to future medical devices, rather than retroactively?

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

Modern FDA Requirements

> (1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;

- ✓ Plans and procedures for Postmarket activities in Premarket submission content
- ✓ Updating, SBOM and other monitoring, incident response, and disclosures and communications



II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-
(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, ...xploits, ...es;
...ide a ...ecure, and ...lated systems ...ble
vulnerabilities; and
(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;
(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and
(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

(c) DEFINITION.—In this section, the term 'cyber device' means a device that—
(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;
(2) has the ability to connect to the internet; and
(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s,[1] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[2] and Acceptance Review for De Novo Classification Requests.[3]

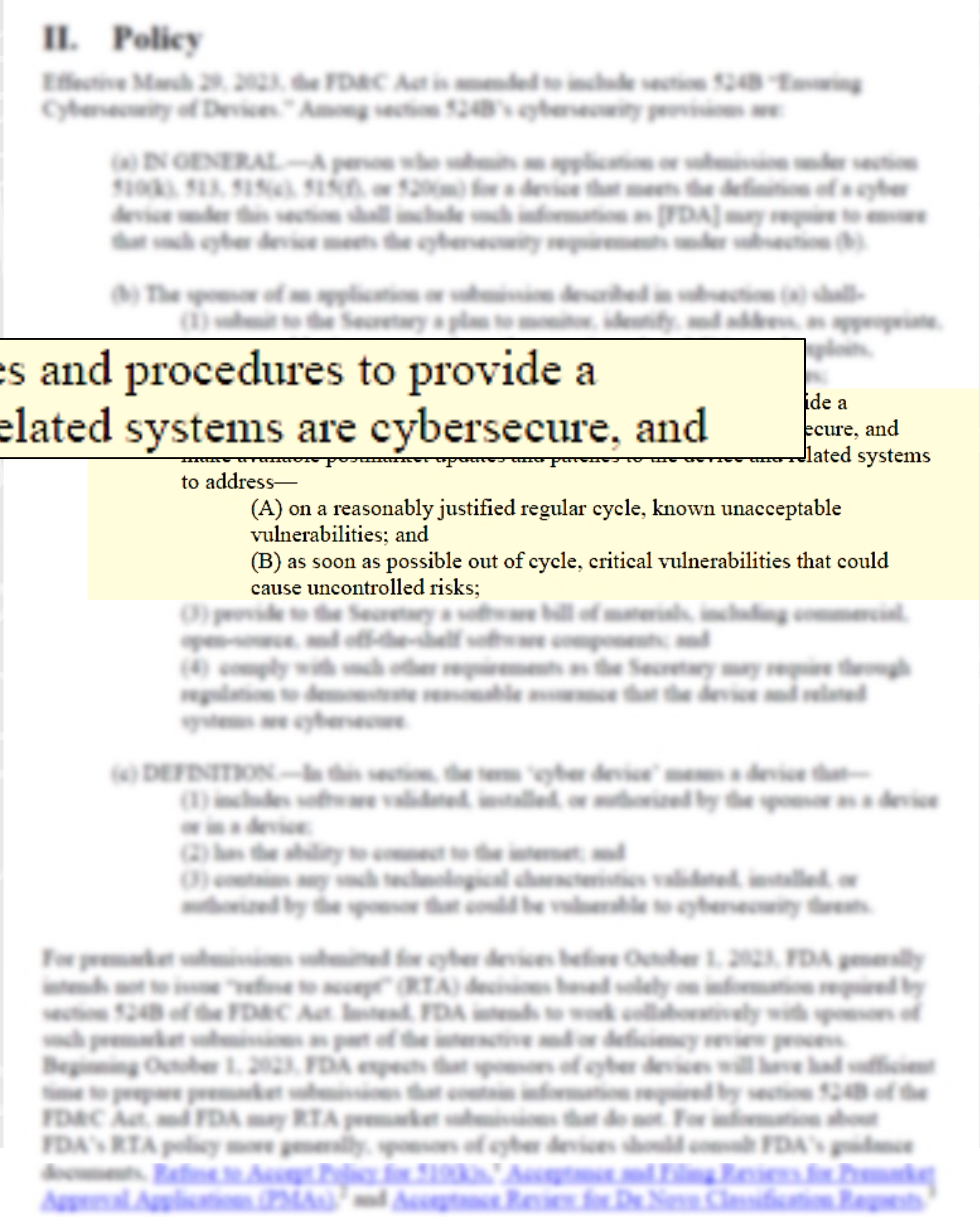
Medical Device Engineering: Your IP. Designed and Built.

VELENTIUM

Modern FDA Requirements

(2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and

- ✓ Plans and procedures for Premarket development activities
- ✓ Reasonable assurance for cybersecurity throughout complete product lifecycle



II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-

(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, … exploits, … es;

… ide a … ecure, and make available postmarket updates and patches to the device and related systems to address—

(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

(c) DEFINITION.—In this section, the term 'cyber device' means a device that—

(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;

(2) has the ability to connect to the internet; and

(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s,[1] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[2] and Acceptance Review for De Novo Classification Requests.[3]

Medical Device Engineering: Your IP. Designed and Built.

VELENTIUM

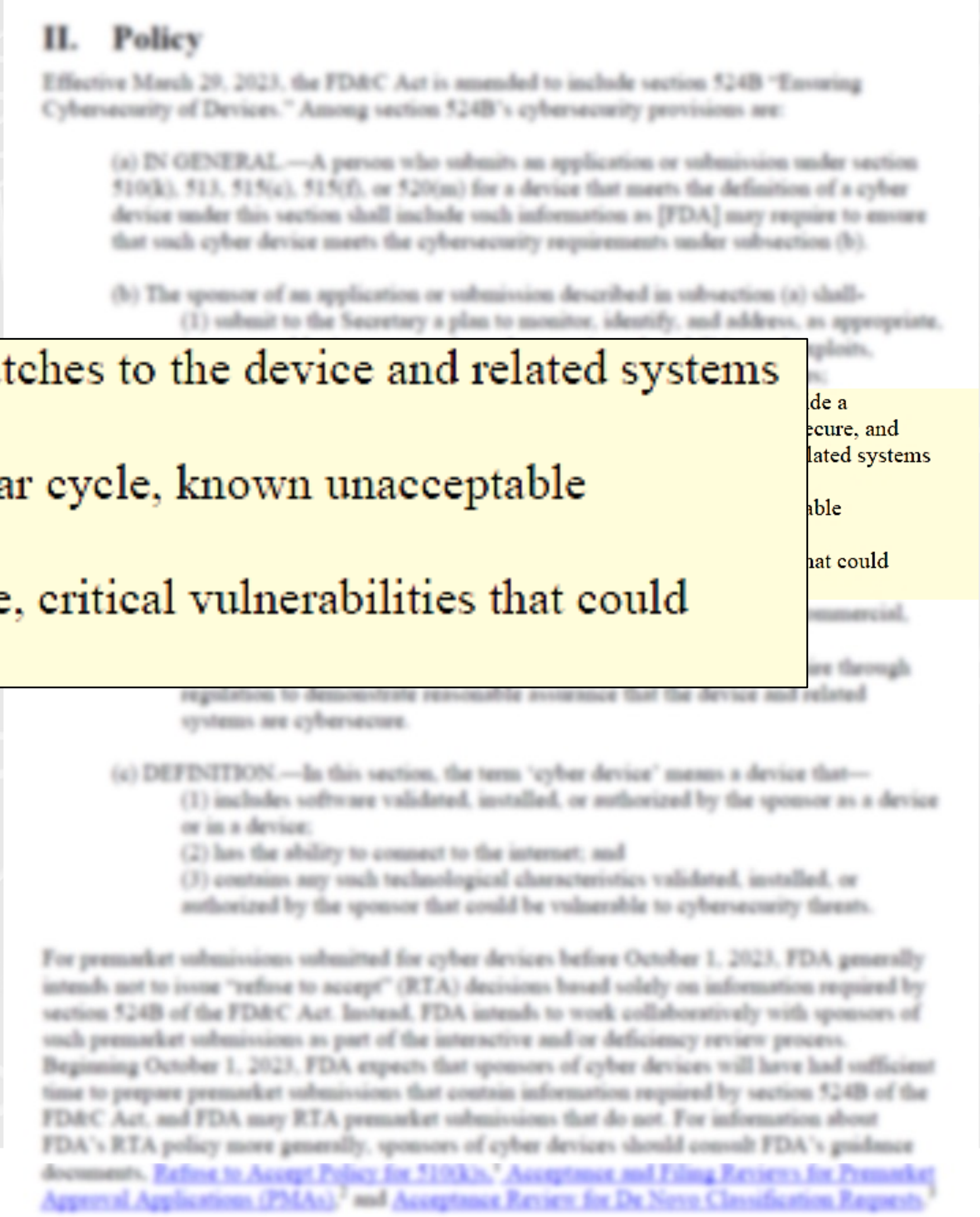
Modern FDA Requirements

make available postmarket updates and patches to the device and related systems to address—

(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

- ✓ Regular update cycles based on platform/device type
- ✓ Timely updates as needed
- ✓ Look to forthcoming Joint Security Plan v2 by HSCC



II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-

(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, … exploits, … s;

… de a … ecure, and … lated systems

… able

… hat could

… commercial, … re through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

(c) DEFINITION.—In this section, the term 'cyber device' means a device that—

(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;

(2) has the ability to connect to the internet; and

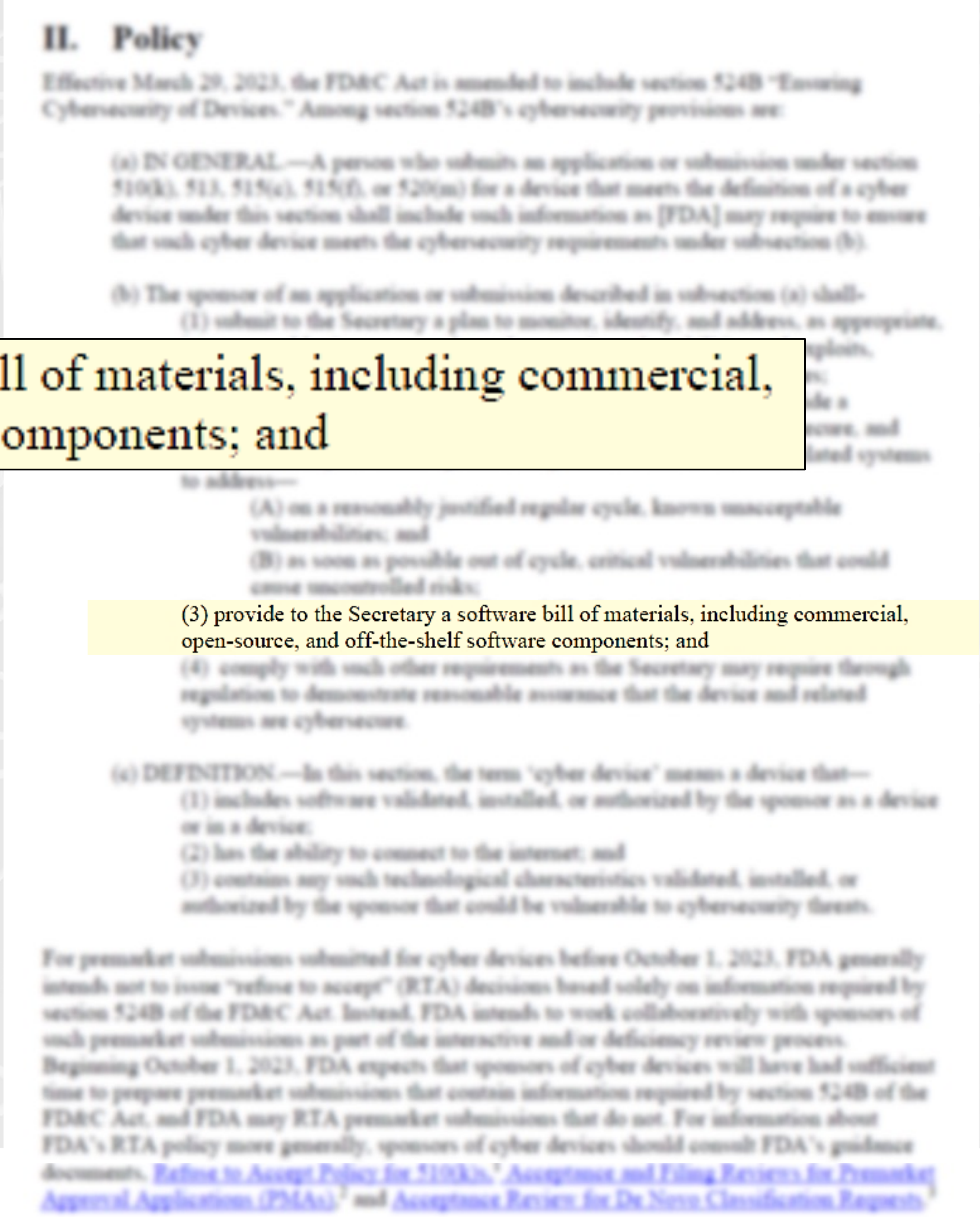
(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s,[1] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[2] and Acceptance Review for De Novo Classification Requests.[3]

Modern FDA Requirements

(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

- ✓ Machine-readable SBOM of all software components and associated processes (maintain, monitor, share)



II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-

(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate,

to address—

(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

(c) DEFINITION.—In this section, the term 'cyber device' means a device that—

(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;

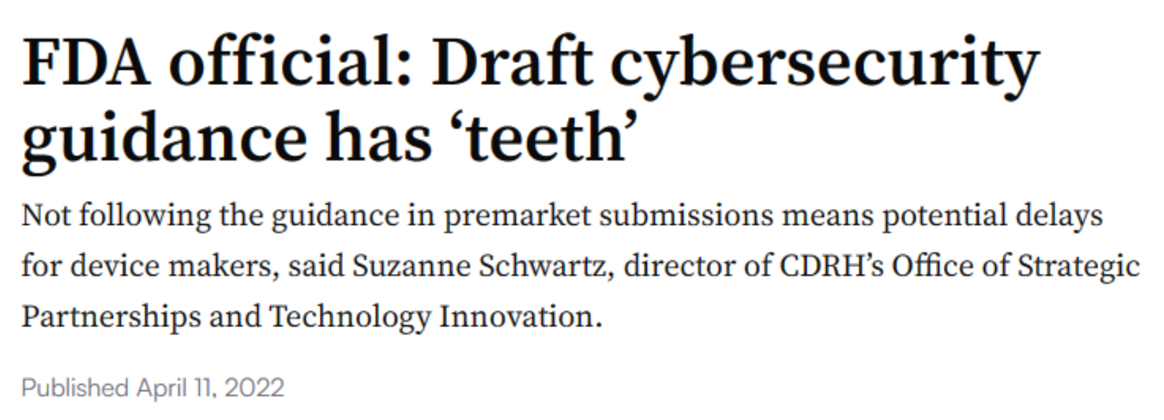
(2) has the ability to connect to the internet; and

(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s,[2] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[3] and Acceptance Review for De Novo Classification Requests.[4]

Modern FDA Requirements

(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

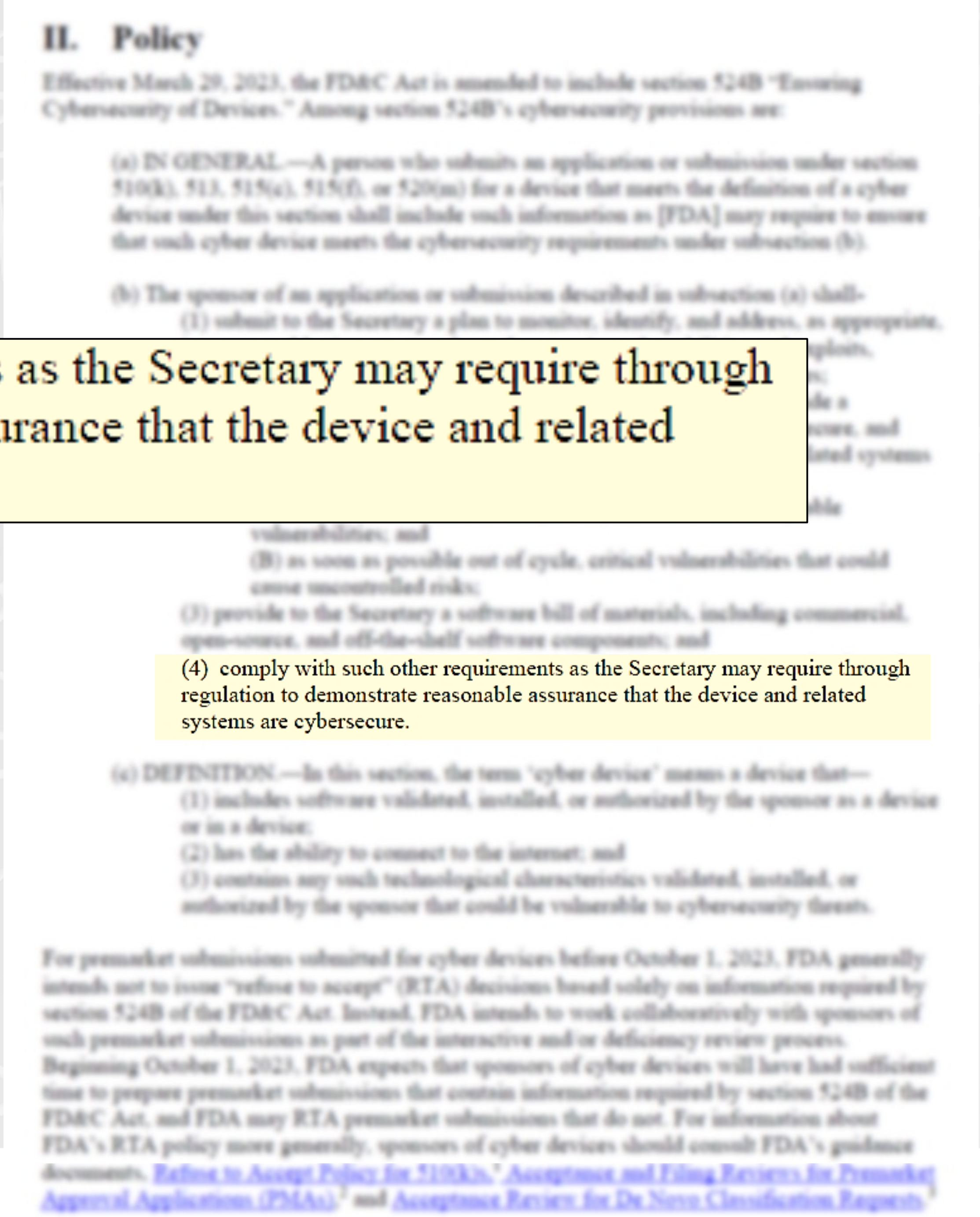


FDA official: Draft cybersecurity guidance has 'teeth'

Not following the guidance in premarket submissions means potential delays for device makers, said Suzanne Schwartz, director of CDRH's Office of Strategic Partnerships and Technology Innovation.

Published April 11, 2022

https://www.medtechdive.com/news/fda-draft-cybersecurity-guidance-requirements/621872/



II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-

(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, ... exploits, ... de a ... cure, and ... lated systems ... ble

vulnerabilities; and

(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

(c) DEFINITION.—In this section, the term 'cyber device' means a device that—

(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;

(2) has the ability to connect to the internet; and

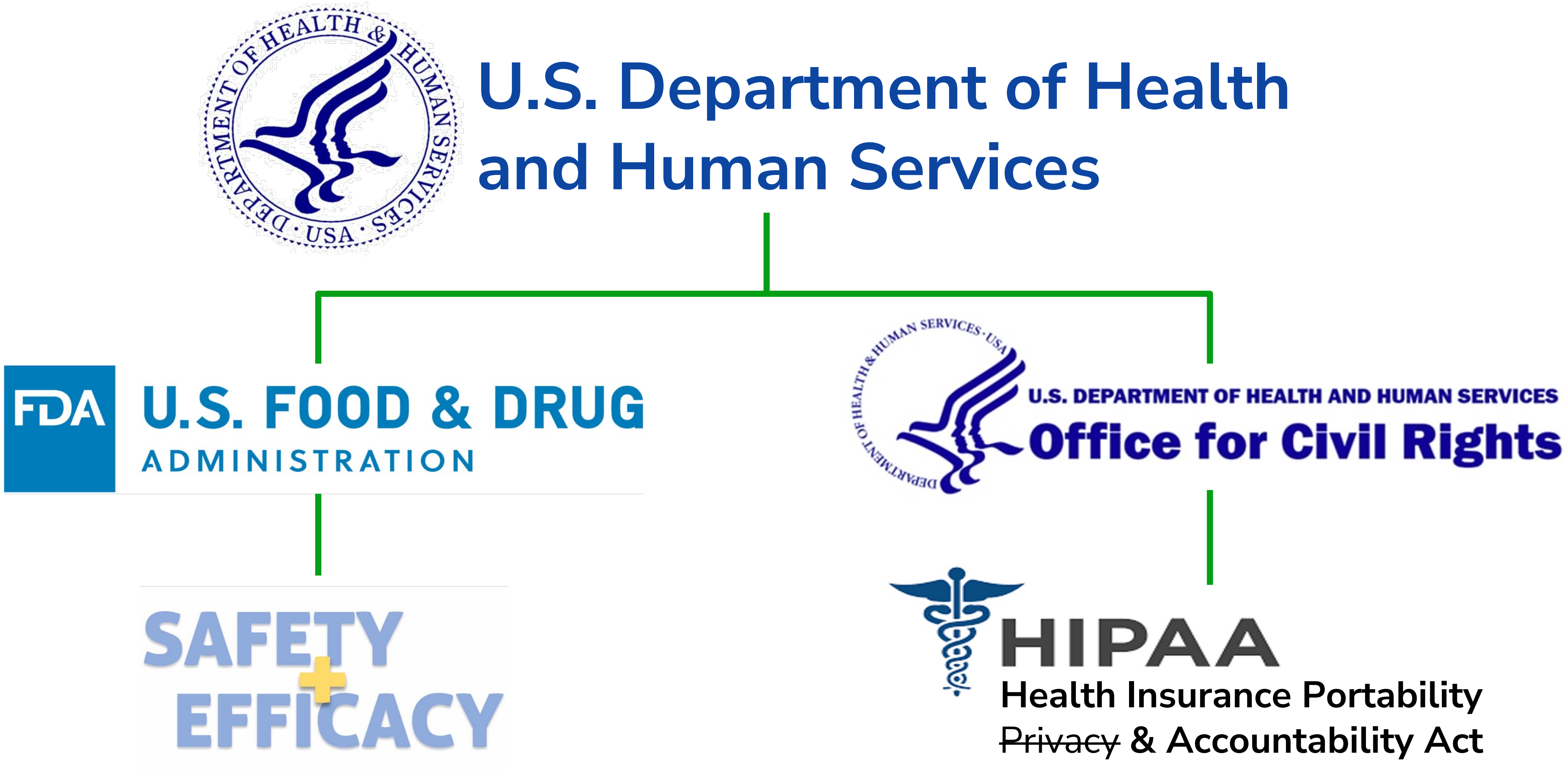
(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s,[1] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[2] and Acceptance Review for De Novo Classification Requests.[3]

Myth:

There must be an explicit link between security and safety for the FDA to have authority

BUSTED



U.S. Department of Health and Human Services

U.S. FOOD & DRUG ADMINISTRATION

SAFETY + EFFICACY

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

HIPAA

Health Insurance Portability ~~Privacy~~ & Accountability Act

“The FDA… ensures that… medical devices are safe and effective…”

“OCR ensures that… individuals can access and trust the privacy and security of their health information.”

https://www.hhs.gov/about/agencies/hhs-agencies-and-offices/index.html

Shifting Sands of MedTech Security

- No longer an explicit link between safety and security required for FDA authority
  - Security alone is enough

- Plus, many other regulatory bodies are joining the party…

HIPAA Violations

- $100 to $250,000 fine per incident
- Largest to-date: $16 million due to data breach
- Common HIPAA violations:
  1. Snooping on Healthcare Records
  2. Failure to Perform an Organization-Wide Risk Analysis
  3. Failure to Manage Security Risks / Lack of a Risk Management Process
  4. Insufficient ePHI Access Controls
  5. Failure to Use Encryption or an Equivalent Measure to Safeguard ePHI on Portable Devices
  6. Exceeding the 60-Day Deadline for Issuing Breach Notifications
  7. Improper Disposal of PHI

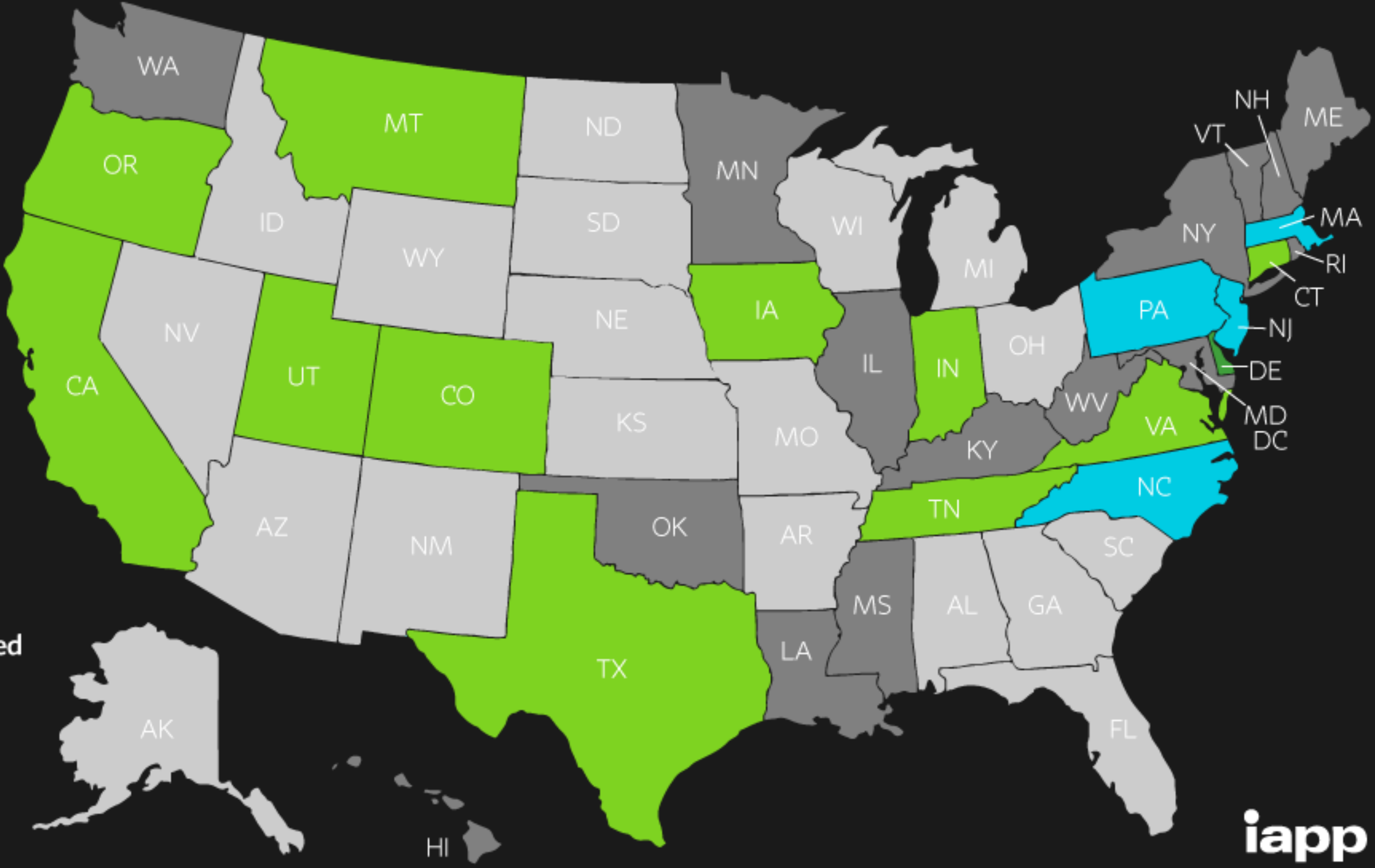
https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

https://www.hipaajournal.com/common-hipaa-violations/

US State Privacy Legislation Tracker 2023

STATUTE/BILL IN LEGISLATIVE PROCESS

- 🟦 Introduced
- 🟦 In committee
- 🟦 In cross chamber
- 🟩 In cross committee
- 🟩 Passed
- 🟩 Signed
- ⬛ Inactive bills
- ⬜ No comprehensive bills introduced

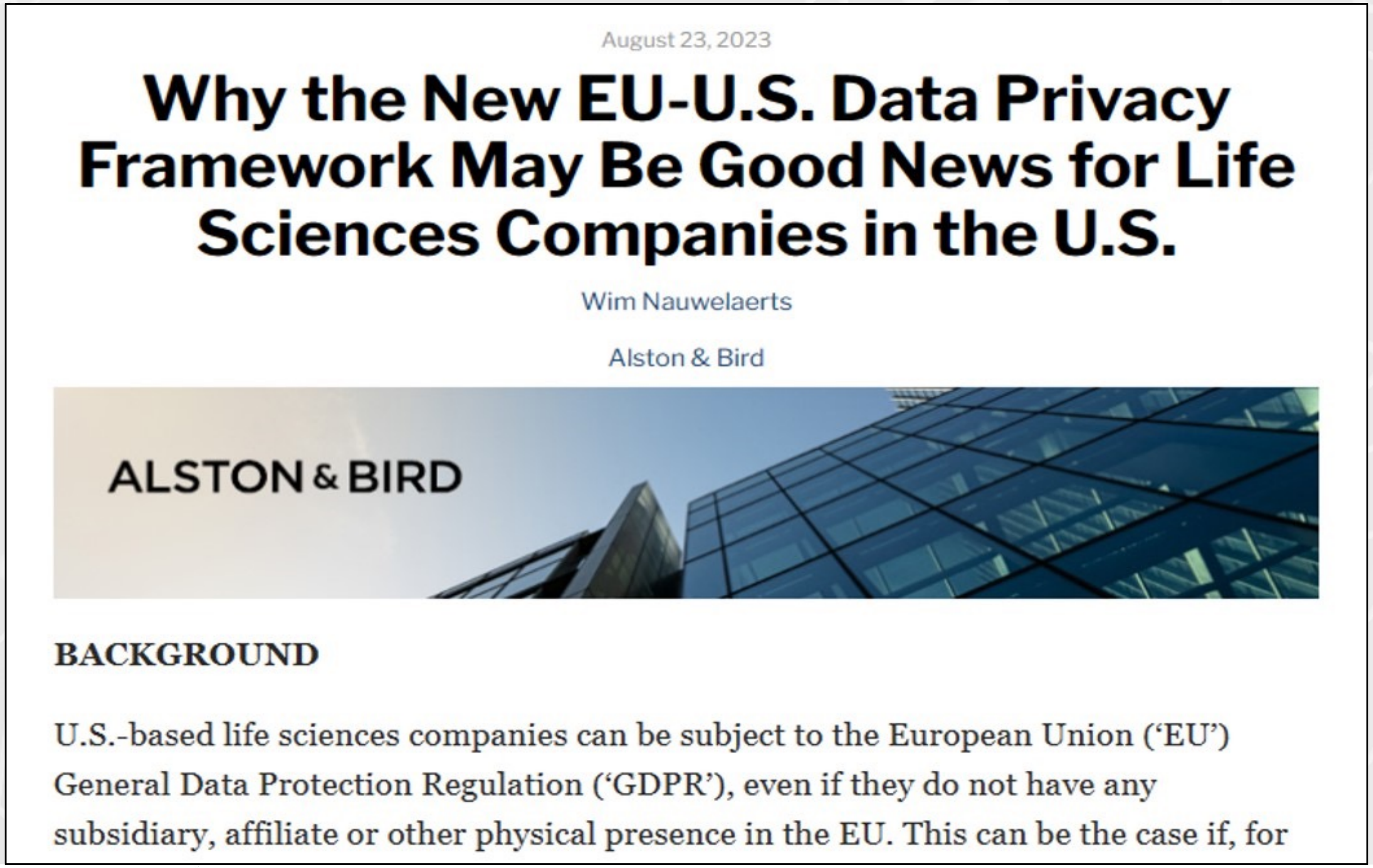


Last updated: 8/4/2023

iapp

https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

General Data Protection Regulation (GDPR)



August 23, 2023

Why the New EU-U.S. Data Privacy Framework May Be Good News for Life Sciences Companies in the U.S.

Wim Nauwelaerts

Alston & Bird

BACKGROUND

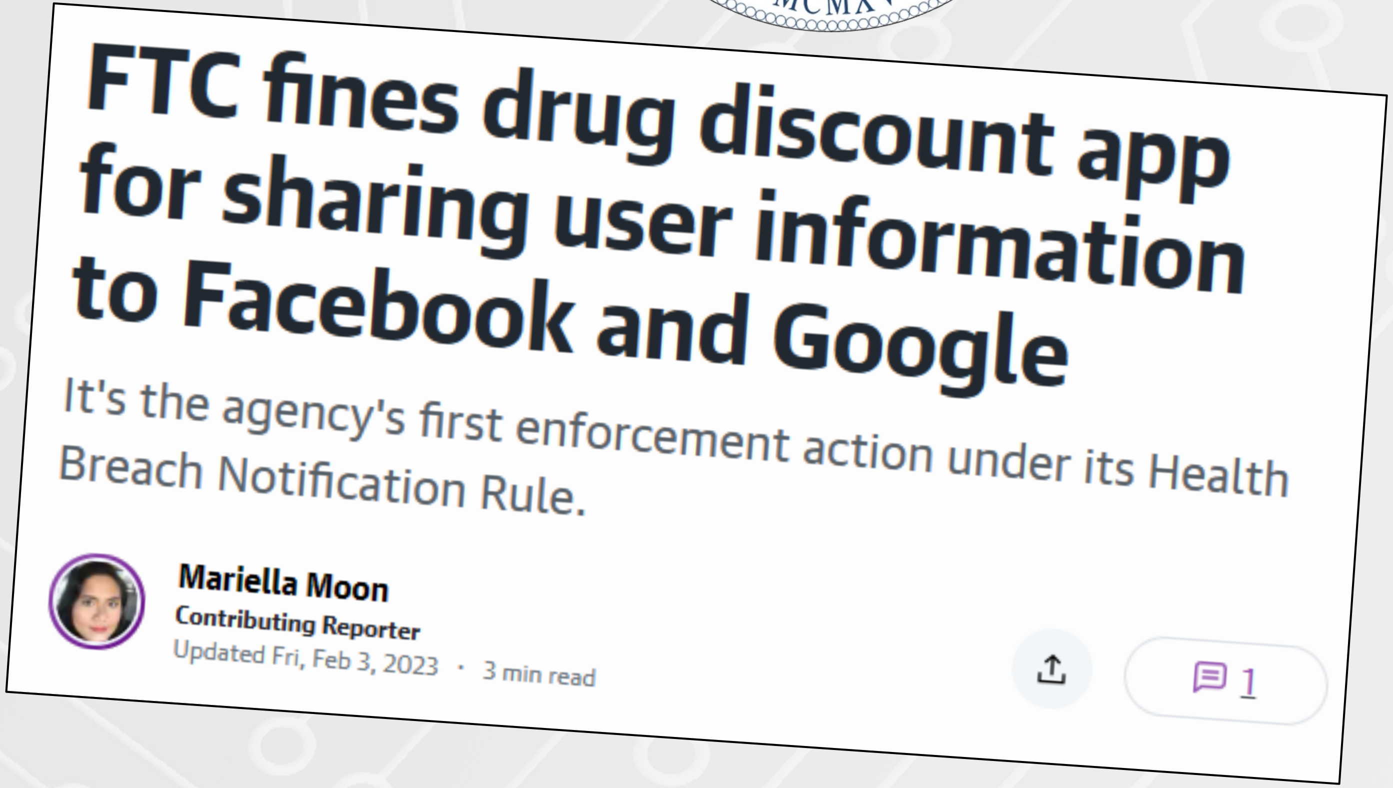
U.S.-based life sciences companies can be subject to the European Union ('EU') General Data Protection Regulation ('GDPR'), even if they do not have any subsidiary, affiliate or other physical presence in the EU. This can be the case if, for

Medical Device Engineering: Your IP. Designed and Built.

https://gdpr.eu/fines/

Federal Trade Commission (FTC)

- Protects consumers’ health privacy
- Focus on large-scale events
- Lawyer up!



FTC fines drug discount app for sharing user information to Facebook and Google

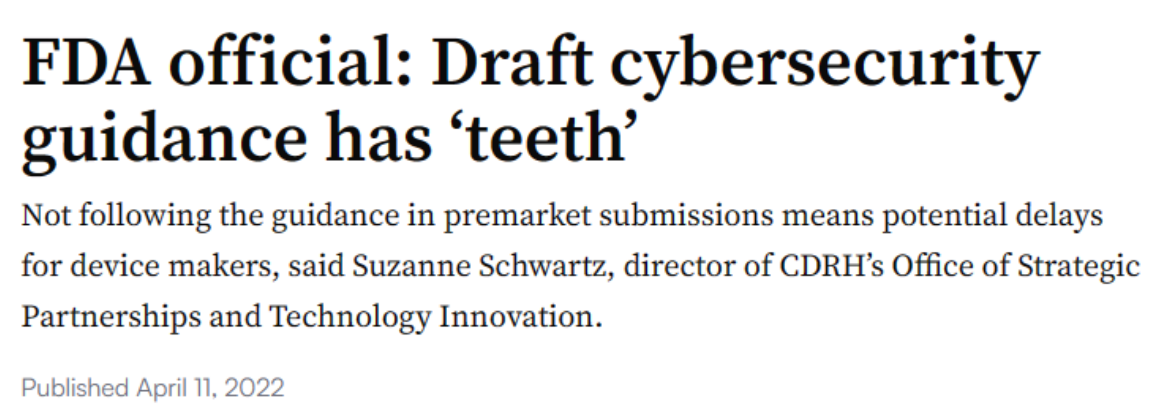
It's the agency's first enforcement action under its Health Breach Notification Rule.

Mariella Moon
Contributing Reporter
Updated Fri, Feb 3, 2023 · 3 min read

https://www.engadget.com/ftc-fines-goodrx-sharing-user-information-facebook-google-045353503.html

Modern FDA Requirements

(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

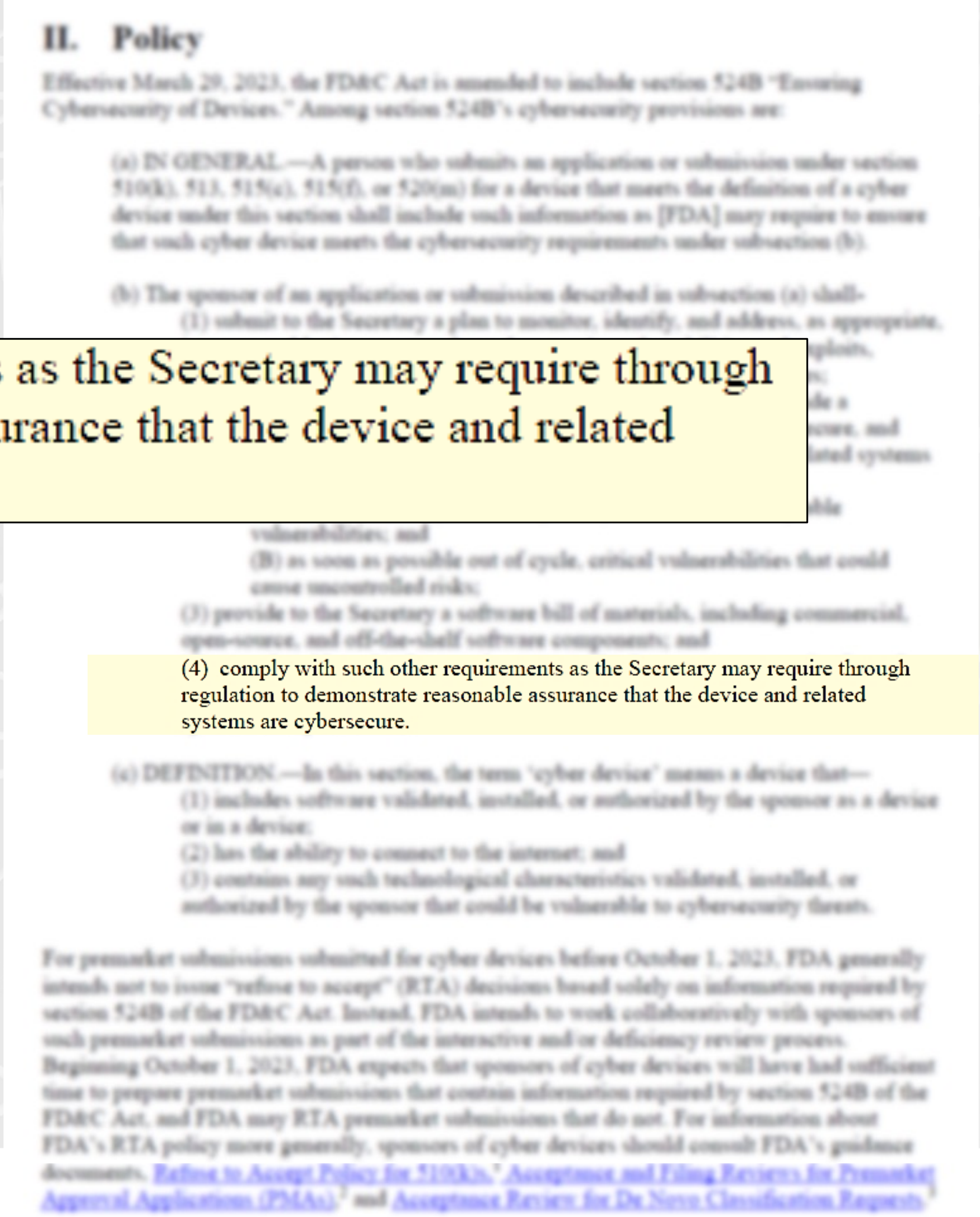


FDA official: Draft cybersecurity guidance has 'teeth'

Not following the guidance in premarket submissions means potential delays for device makers, said Suzanne Schwartz, director of CDRH's Office of Strategic Partnerships and Technology Innovation.

Published April 11, 2022

https://www.medtechdive.com/news/fda-draft-cybersecurity-guidance-requirements/621872/



II. Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-
(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate,
ploits,
s;
de a
ecure, and
lated systems
ble
vulnerabilities; and
(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;
(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

(c) DEFINITION.—In this section, the term 'cyber device' means a device that—
(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;
(2) has the ability to connect to the internet; and
(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

For premarket submissions submitted for cyber devices before October 1, 2023, FDA generally intends not to issue "refuse to accept" (RTA) decisions based solely on information required by section 524B of the FD&C Act. Instead, FDA intends to work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. Beginning October 1, 2023, FDA expects that sponsors of cyber devices will have had sufficient time to prepare premarket submissions that contain information required by section 524B of the FD&C Act, and FDA may RTA premarket submissions that do not. For information about FDA's RTA policy more generally, sponsors of cyber devices should consult FDA's guidance documents, Refuse to Accept Policy for 510(k)s,[7] Acceptance and Filing Reviews for Premarket Approval Applications (PMAs),[7] and Acceptance Review for De Novo Classification Requests.[3]

Myth:

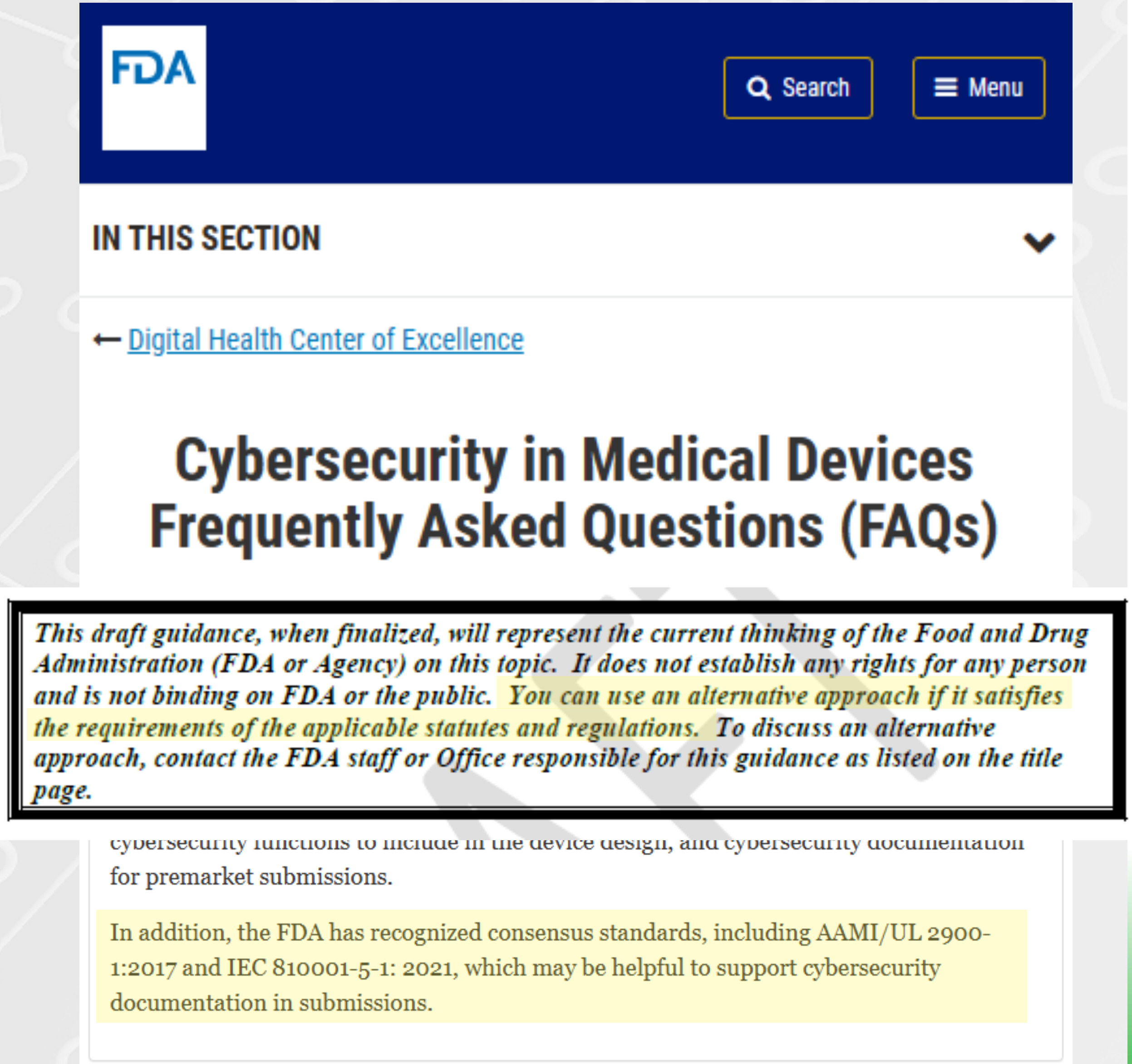
The Premarket Guidance must be followed verbatim

BUSTED

Medical Device Engineering: Your IP. Designed and Built.

Guidance

- FDA's opinion of easiest path to demonstrate reasonable assurance of cybersecurity to them
- MDMs do not necessarily have to follow this but will then have to justify their decisions
- Make your life easier with recognized standards and the discussed documentation



Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)

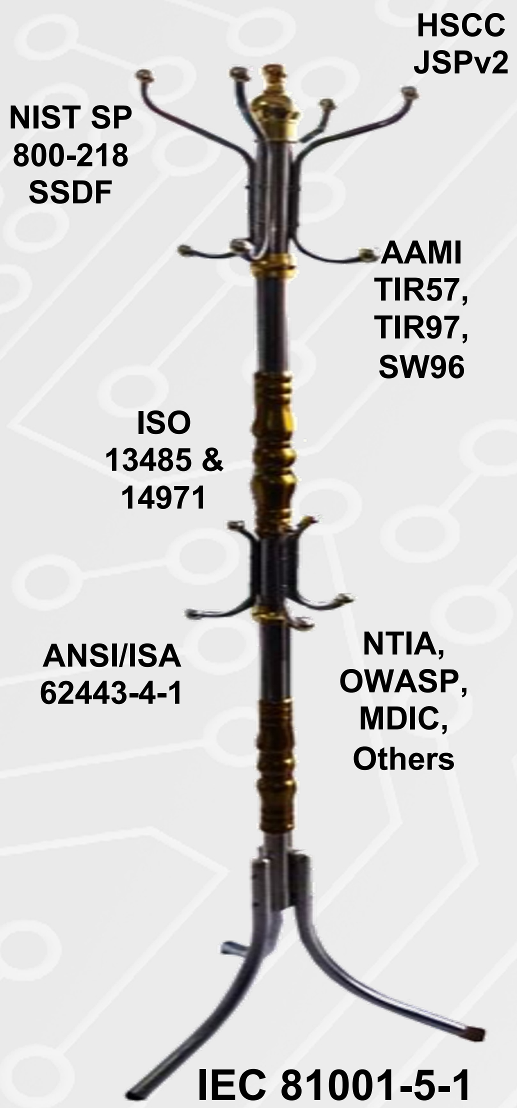
This draft guidance, when finalized, will represent the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

cybersecurity functions to include in the device design, and cybersecurity documentation for premarket submissions.

In addition, the FDA has recognized consensus standards, including AAMI/UL 2900-1:2017 and IEC 810001-5-1: 2021, which may be helpful to support cybersecurity documentation in submissions.

Secure Product Development Framework

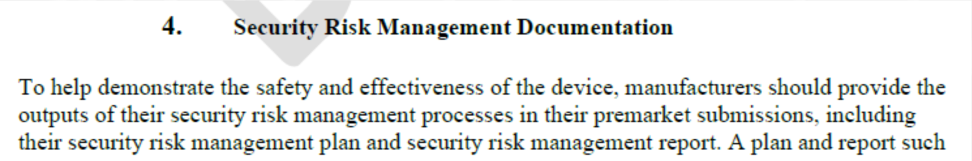
- Heavy plan and procedure requirements
- IEC 81001-5-1:2021 Activities in the product life cycle
- Many other frameworks to build off of IEC 81001 for SPDF



https://www.iso.org/standard/76097.html

2022 Draft Premarket Requirements

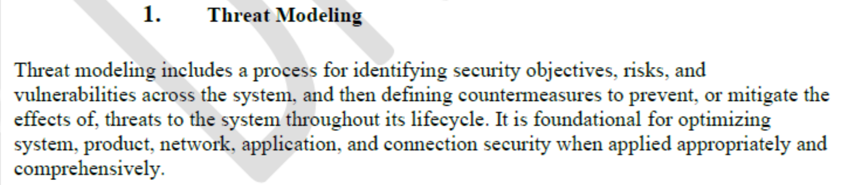
- Security Risk Management Plan
  - Including Pre- & Postmarket activities
- Threat Modeling
  - System wide plus supply chain, transfer, deployment, updating, decommissioning
- Security Requirements
- Security Architecture
  - Security Architecture Views of global system, multi-patient harm, updating, security use cases
- SBOM Generation & Processes
- Commercial Device/OS Hardening
- MDM Configuration & Deployment



4. Security Risk Management Documentation

To help demonstrate the safety and effectiveness of the device, manufacturers should provide the outputs of their security risk management processes in their premarket submissions, including their security risk management plan and security risk management report. A plan and report such

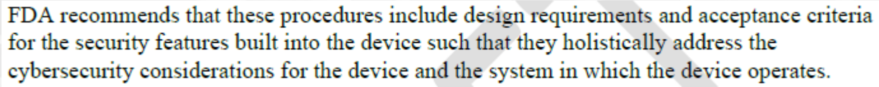
Section V.A.4. (pages 14-15)



1. Threat Modeling

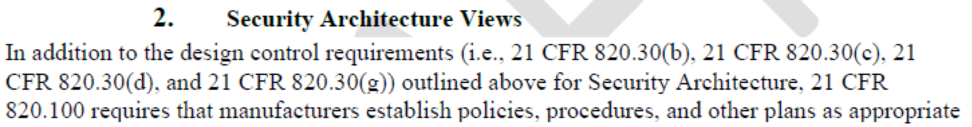
Threat modeling includes a process for identifying security objectives, risks, and vulnerabilities across the system, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system throughout its lifecycle. It is foundational for optimizing system, product, network, application, and connection security when applied appropriately and comprehensively.

Section V.A.1. (page 10)



FDA recommends that these procedures include design requirements and acceptance criteria for the security features built into the device such that they holistically address the cybersecurity considerations for the device and the system in which the device operates.

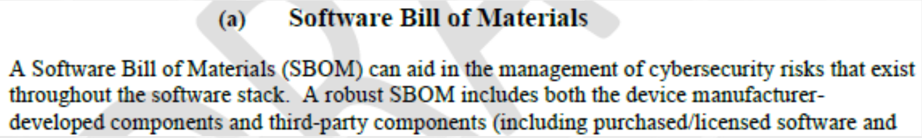
Section V.B.1. (pages 17-18)



2. Security Architecture Views

In addition to the design control requirements (i.e., 21 CFR 820.30(b), 21 CFR 820.30(c), 21 CFR 820.30(d), and 21 CFR 820.30(g)) outlined above for Security Architecture, 21 CFR 820.100 requires that manufacturers establish policies, procedures, and other plans as appropriate

Section V.B.2. (pages 19-22)



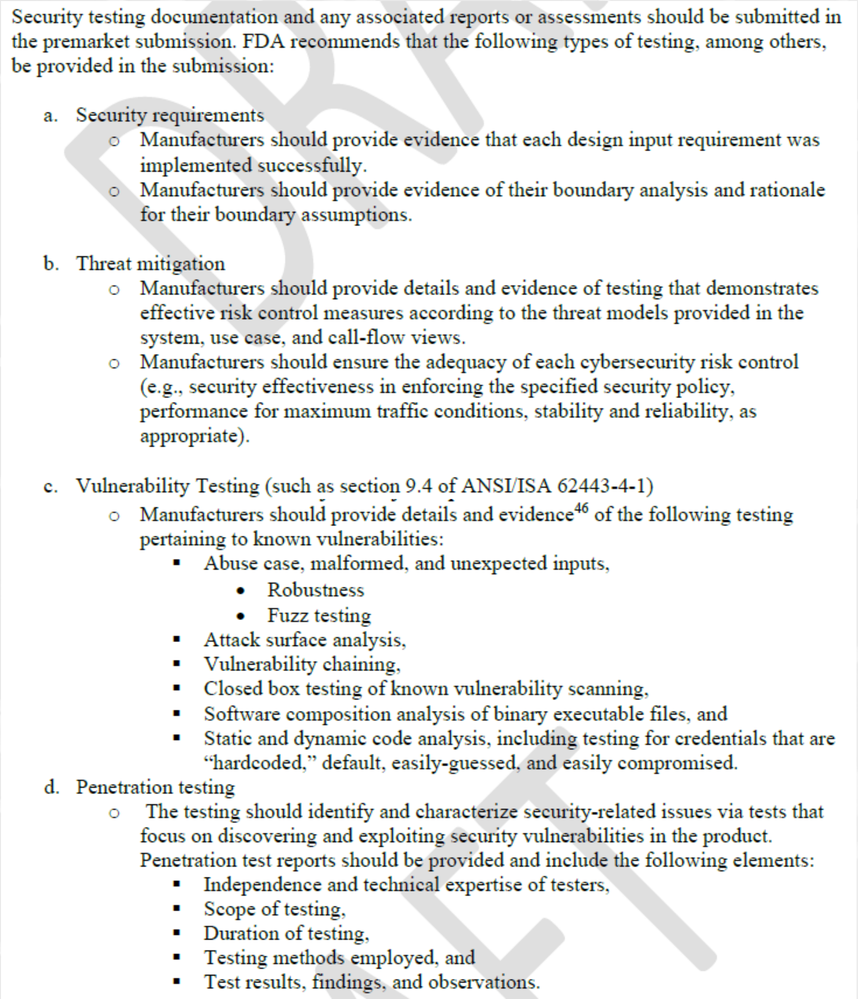
(a) Software Bill of Materials

A Software Bill of Materials (SBOM) can aid in the management of cybersecurity risks that exist throughout the software stack. A robust SBOM includes both the device manufacturer-developed components and third-party components (including purchased/licensed software and

Section V.A.2. (pages 11-14)

2022 Draft Premarket Requirements

- Security Testing
  - Attack Surface Analysis
  - Vulnerability Scanning/Testing
  - Configuration Assessment
  - Static Analysis Security Testing
  - Software Anomaly Testing
  - Malformed Input and Fuzz Testing
  - Penetration Testing
  - Coexistence of Performance & Mitigations Testing
  - Effectiveness of Controls Testing



Security testing documentation and any associated reports or assessments should be submitted in the premarket submission. FDA recommends that the following types of testing, among others, be provided in the submission:

a. Security requirements
   - Manufacturers should provide evidence that each design input requirement was implemented successfully.
   - Manufacturers should provide evidence of their boundary analysis and rationale for their boundary assumptions.

b. Threat mitigation
   - Manufacturers should provide details and evidence of testing that demonstrates effective risk control measures according to the threat models provided in the system, use case, and call-flow views.
   - Manufacturers should ensure the adequacy of each cybersecurity risk control (e.g., security effectiveness in enforcing the specified security policy, performance for maximum traffic conditions, stability and reliability, as appropriate).

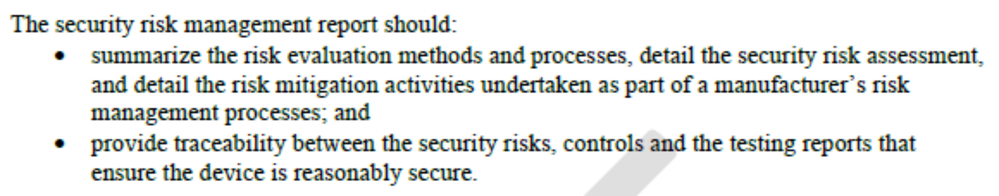
c. Vulnerability Testing (such as section 9.4 of ANSI/ISA 62443-4-1)
   - Manufacturers should provide details and evidence[46] of the following testing pertaining to known vulnerabilities:
     - Abuse case, malformed, and unexpected inputs,
       - Robustness
       - Fuzz testing
     - Attack surface analysis,
     - Vulnerability chaining,
     - Closed box testing of known vulnerability scanning,
     - Software composition analysis of binary executable files, and
     - Static and dynamic code analysis, including testing for credentials that are "hardcoded," default, easily-guessed, and easily compromised.

d. Penetration testing
   - The testing should identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product. Penetration test reports should be provided and include the following elements:
     - Independence and technical expertise of testers,
     - Scope of testing,
     - Duration of testing,
     - Testing methods employed, and
     - Test results, findings, and observations.

Section V.C. (pages 22-24)

2022 Draft Premarket Requirements

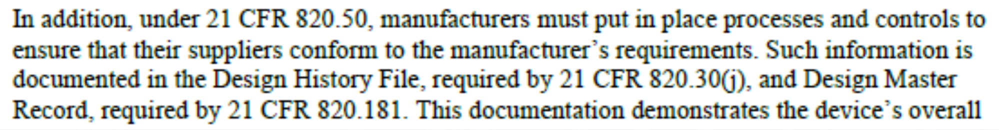
- Cybersecurity Traceability
    - Security Risks, Controls & Testing
- Supply Chain Vendor Cybersecurity Assessment
- Third-Party Component Management & Mitigating Controls
- Security Content for IFU / Labeling
- MDS2 Form
- Security Risk Management Report



The security risk management report should:

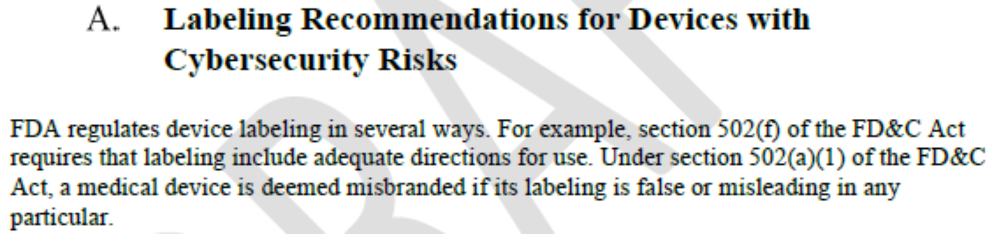
- summarize the risk evaluation methods and processes, detail the security risk assessment, and detail the risk mitigation activities undertaken as part of a manufacturer's risk management processes; and
- provide traceability between the security risks, controls and the testing reports that ensure the device is reasonably secure.

Section V.A.4. (page 15)



In addition, under 21 CFR 820.50, manufacturers must put in place processes and controls to ensure that their suppliers conform to the manufacturer's requirements. Such information is documented in the Design History File, required by 21 CFR 820.30(j), and Design Master Record, required by 21 CFR 820.181. This documentation demonstrates the device's overall

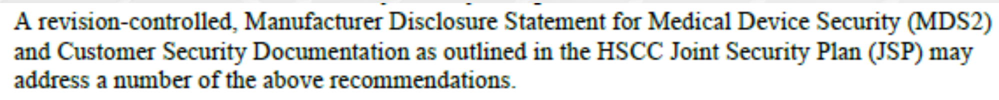
Section V.A.2. (pages 11-14)



A. **Labeling Recommendations for Devices with Cybersecurity Risks**

FDA regulates device labeling in several ways. For example, section 502(f) of the FD&C Act requires that labeling include adequate directions for use. Under section 502(a)(1) of the FD&C Act, a medical device is deemed misbranded if its labeling is false or misleading in any particular.

Section VI.A. (pages 24-25)



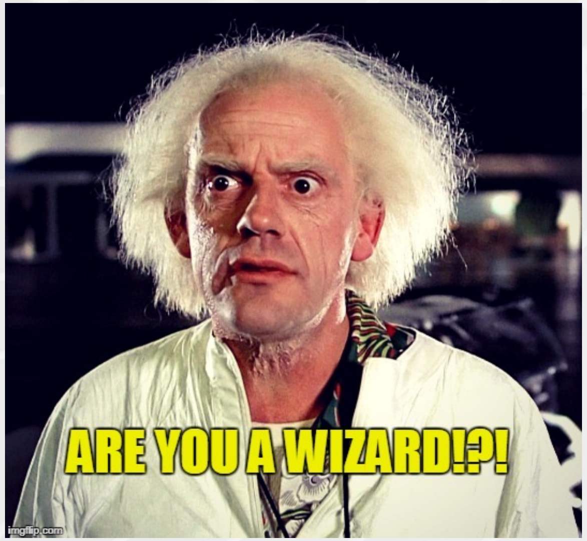
A revision-controlled, Manufacturer Disclosure Statement for Medical Device Security (MDS2) and Customer Security Documentation as outlined in the HSCC Joint Security Plan (JSP) may address a number of the above recommendations.

Section VI.A. (pages 26)

Medical Device Engineering: Your IP. Designed and Built.

To the Future

- Expecting final premarket guidance to be updated in a matter of weeks
  - Language to change but content to remain similar
- Additional eSTAR updates shortly after
- Annual cadence of FDA and CISA working together to define current best practices
- Forthcoming Postmarket guidance updates



THANK YOU

Medical Device Engineering: Your IP. Designed and Built.

Threat Modeling

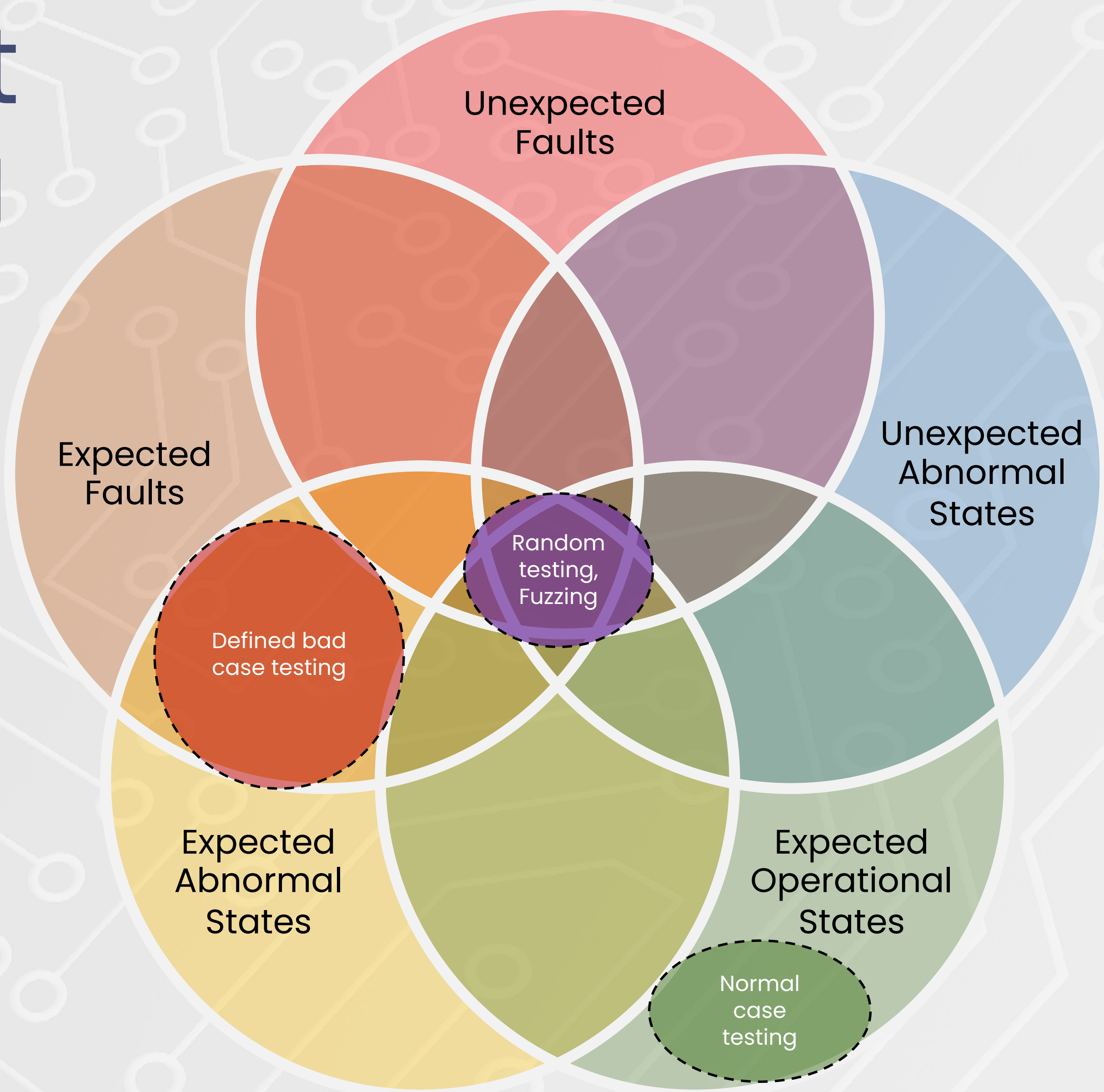
1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

THREAT MODELING MANIFESTO

https://www.threatmodelingmanifesto.org/

Malformed Input and Fuzz Testing

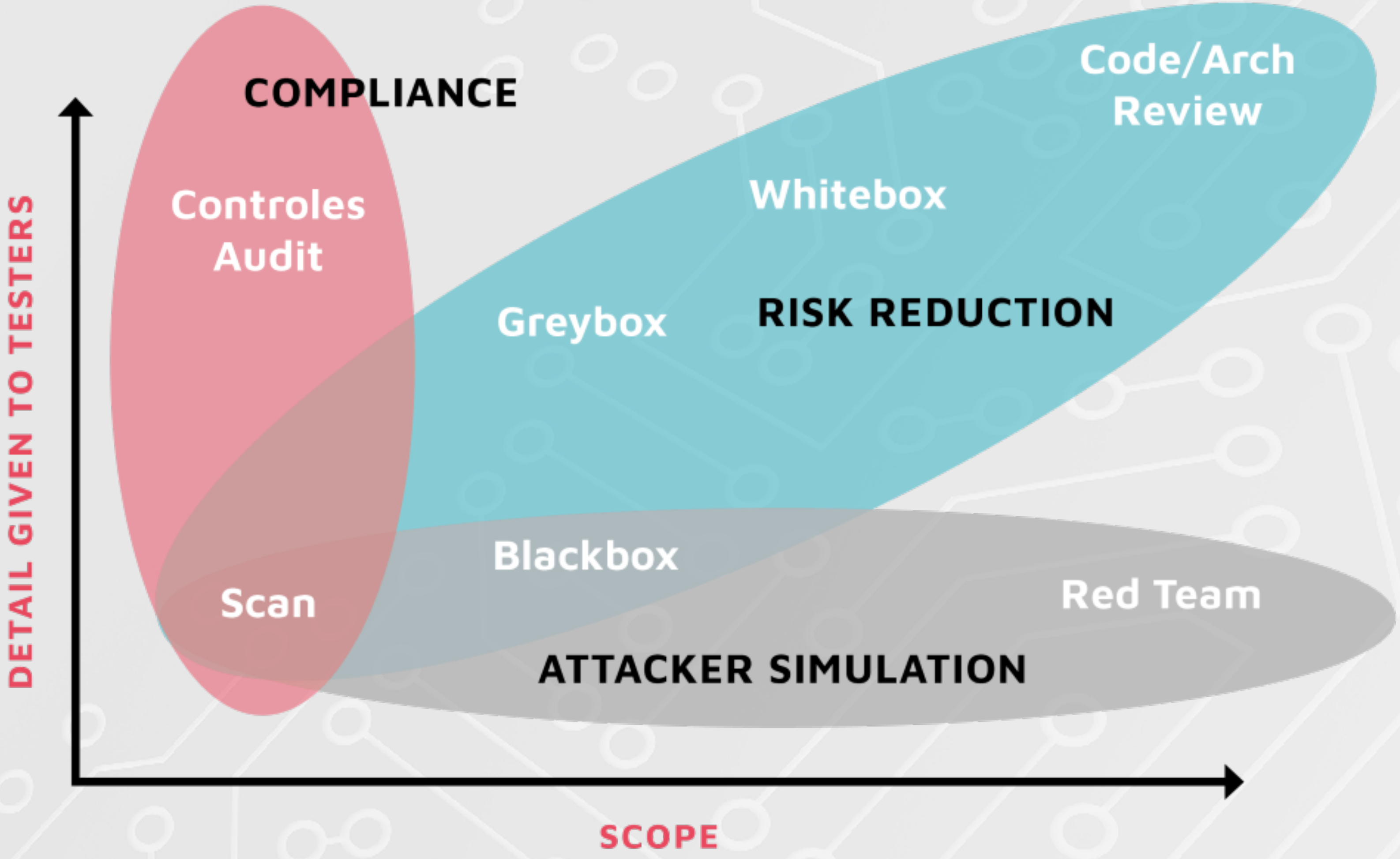
- Injecting malformed, invalid or unexpected inputs into systems
- "Zero-day" discovery
- Robustness testing



Medical Device Engineering: Your IP. Designed and Built.

https://www.intel.com/content/www/us/en/developer/articles/technical/the-schiaparelli-lesson-unusual-and-faulty-conditions.html

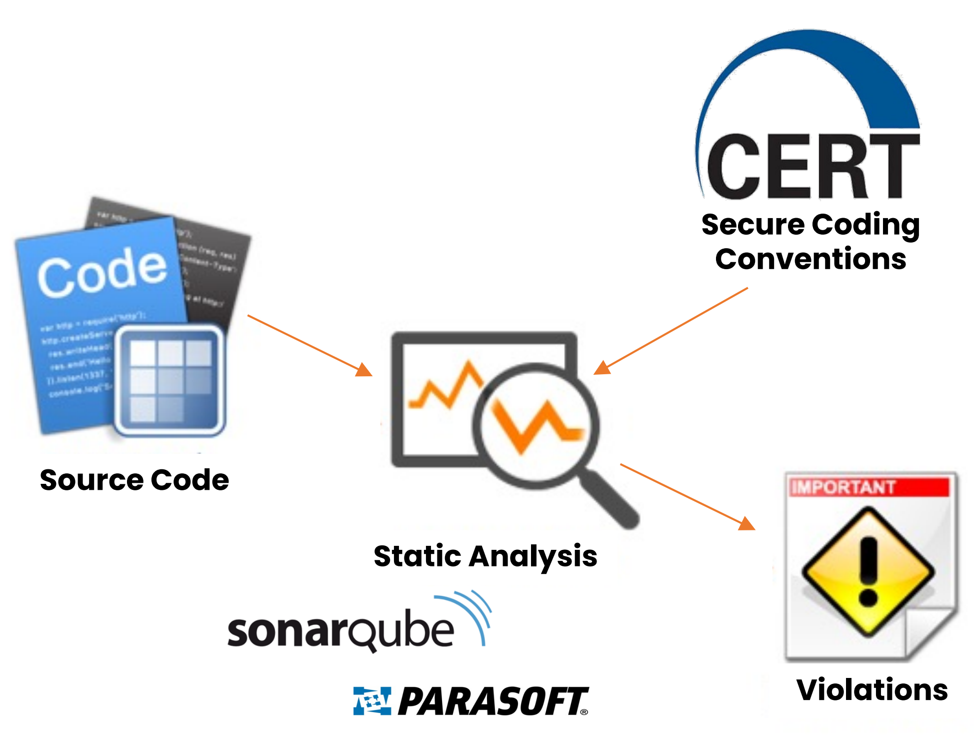
Penetration Testing, Hardening, Configuration Assessment and More…



Medical Device Engineering: Your IP. Designed and Built.

Secure Code Static Analysis

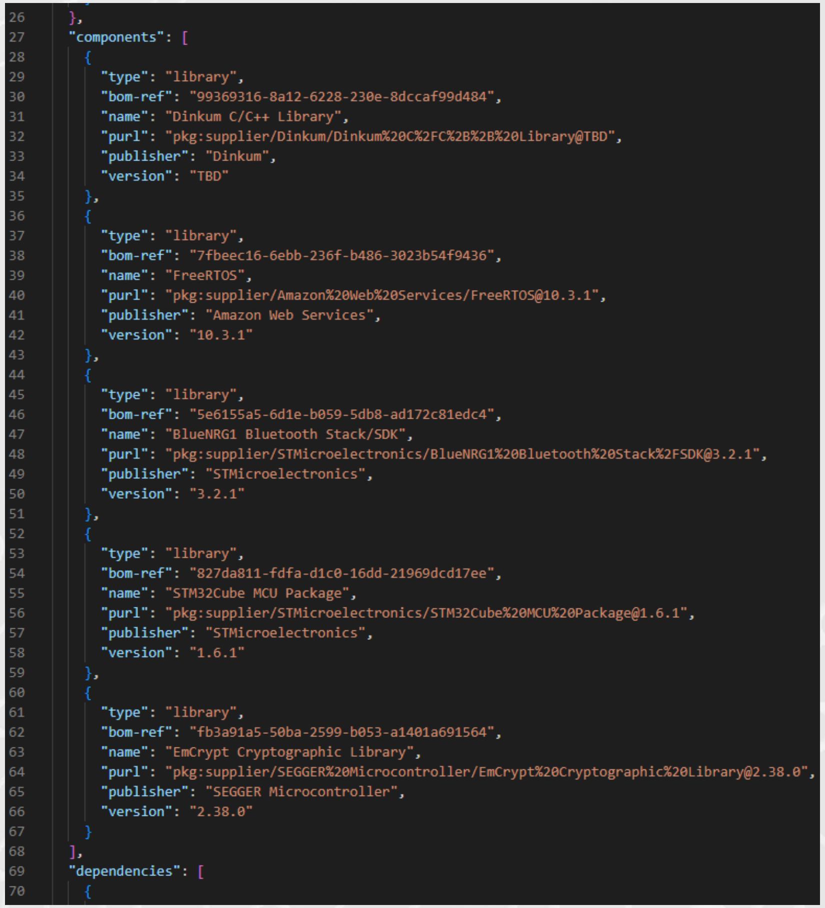
- 93 billion lines of code written in 2020
  - Out of ~3 trillion lines total
- Errors per 1000 lines of code
  - Industry average 15-50 per 1000
  - The “best” teams get to 1-5 per 1000
- So lets call it 10 per 1000…
  - 30 billion bugs ever written!
  - 930 million bugs created in 2020 alone



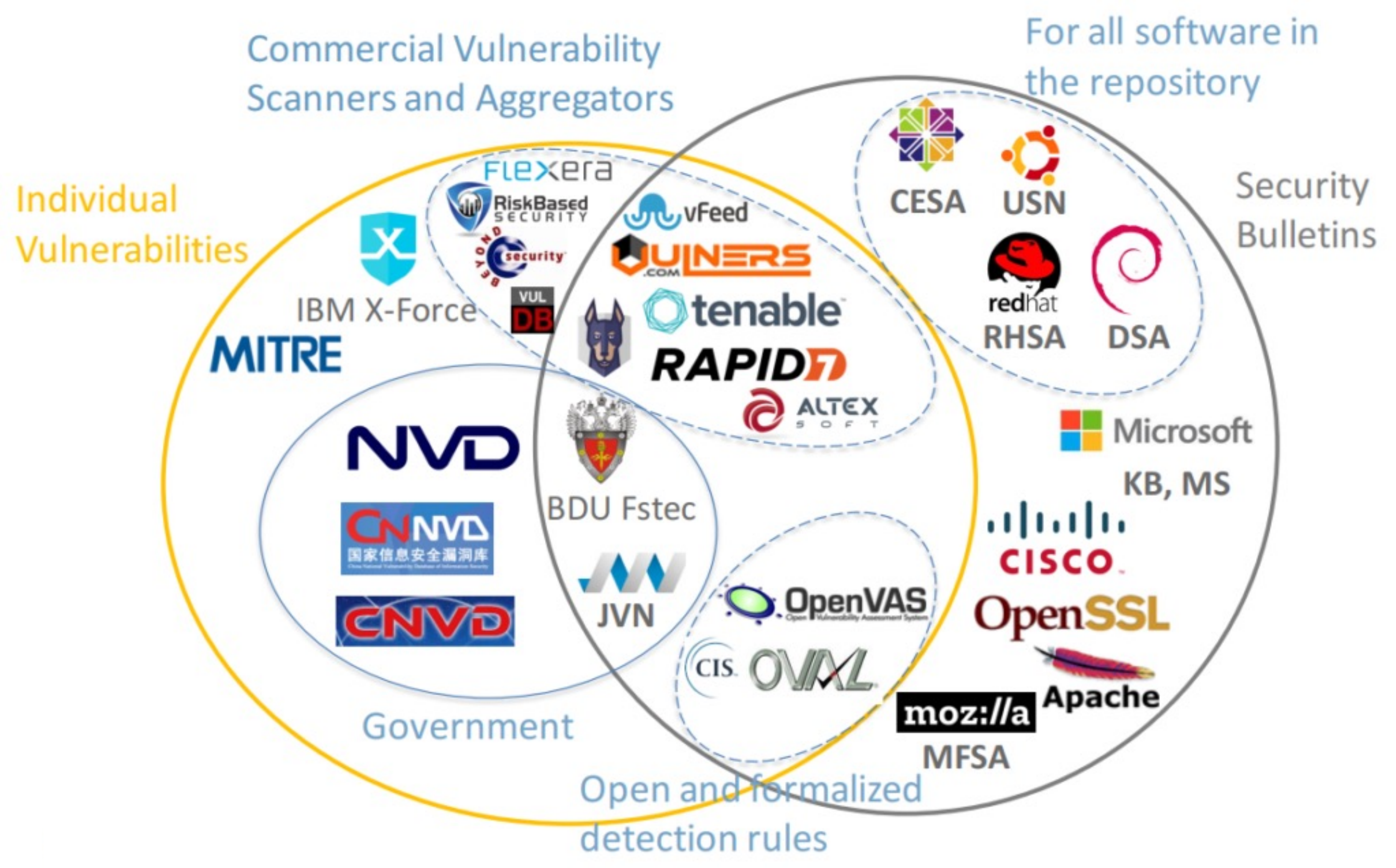
Medical Device Engineering: Your IP. Designed and Built.

https://www.linkedin.com/posts/sidragon1_devsecops-research-microsoft-activity-6890937687423950848-VM_W/

SBOMs & Post-Market Surveillance

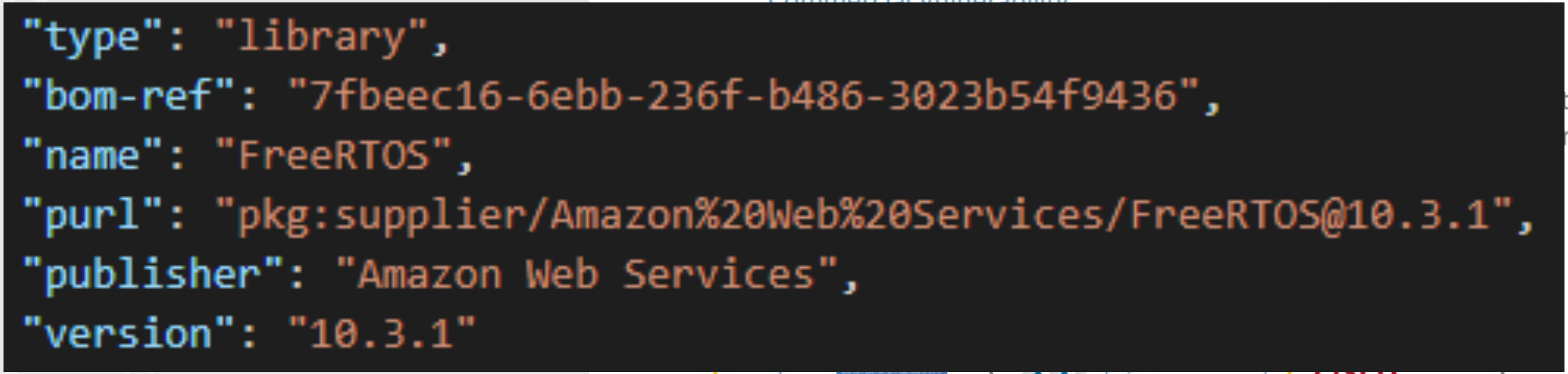


```
  },
  "components": [
    {
      "type": "library",
      "bom-ref": "99369316-8a12-6228-230e-8dccaf99d484",
      "name": "Dinkum C/C++ Library",
      "purl": "pkg:supplier/Dinkum/Dinkum%20C%2FC%2B%2B%20Library@TBD",
      "publisher": "Dinkum",
      "version": "TBD"
    },
    {
      "type": "library",
      "bom-ref": "7fbeec16-6ebb-236f-b486-3023b54f9436",
      "name": "FreeRTOS",
      "purl": "pkg:supplier/Amazon%20Web%20Services/FreeRTOS@10.3.1",
      "publisher": "Amazon Web Services",
      "version": "10.3.1"
    },
    {
      "type": "library",
      "bom-ref": "5e6155a5-6d1e-b059-5db8-ad172c81edc4",
      "name": "BlueNRG1 Bluetooth Stack/SDK",
      "purl": "pkg:supplier/STMicroelectronics/BlueNRG1%20Bluetooth%20Stack%2FSDK@3.2.1",
      "publisher": "STMicroelectronics",
      "version": "3.2.1"
    },
    {
      "type": "library",
      "bom-ref": "827da811-fdfa-d1c0-16dd-21969dcd17ee",
      "name": "STM32Cube MCU Package",
      "purl": "pkg:supplier/STMicroelectronics/STM32Cube%20MCU%20Package@1.6.1",
      "publisher": "STMicroelectronics",
      "version": "1.6.1"
    },
    {
      "type": "library",
      "bom-ref": "fb3a91a5-50ba-2599-b053-a1401a691564",
      "name": "EmCrypt Cryptographic Library",
      "purl": "pkg:supplier/SEGGER%20Microcontroller/EmCrypt%20Cryptographic%20Library@2.38.0",
      "publisher": "SEGGER Microcontroller",
      "version": "2.38.0"
    }
  ],
  "dependencies": [
    {
```

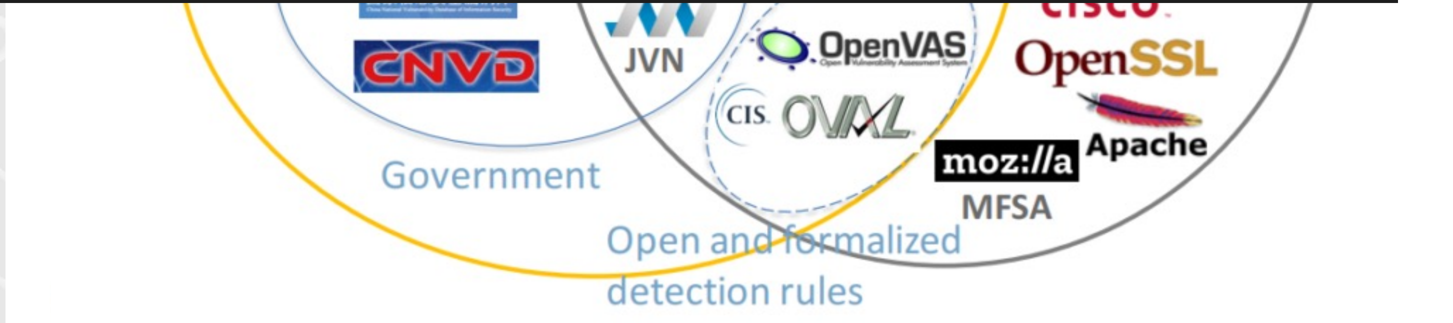


https://avleonov.com/2018/06/05/vulnerability-databases-classification-and-registry/

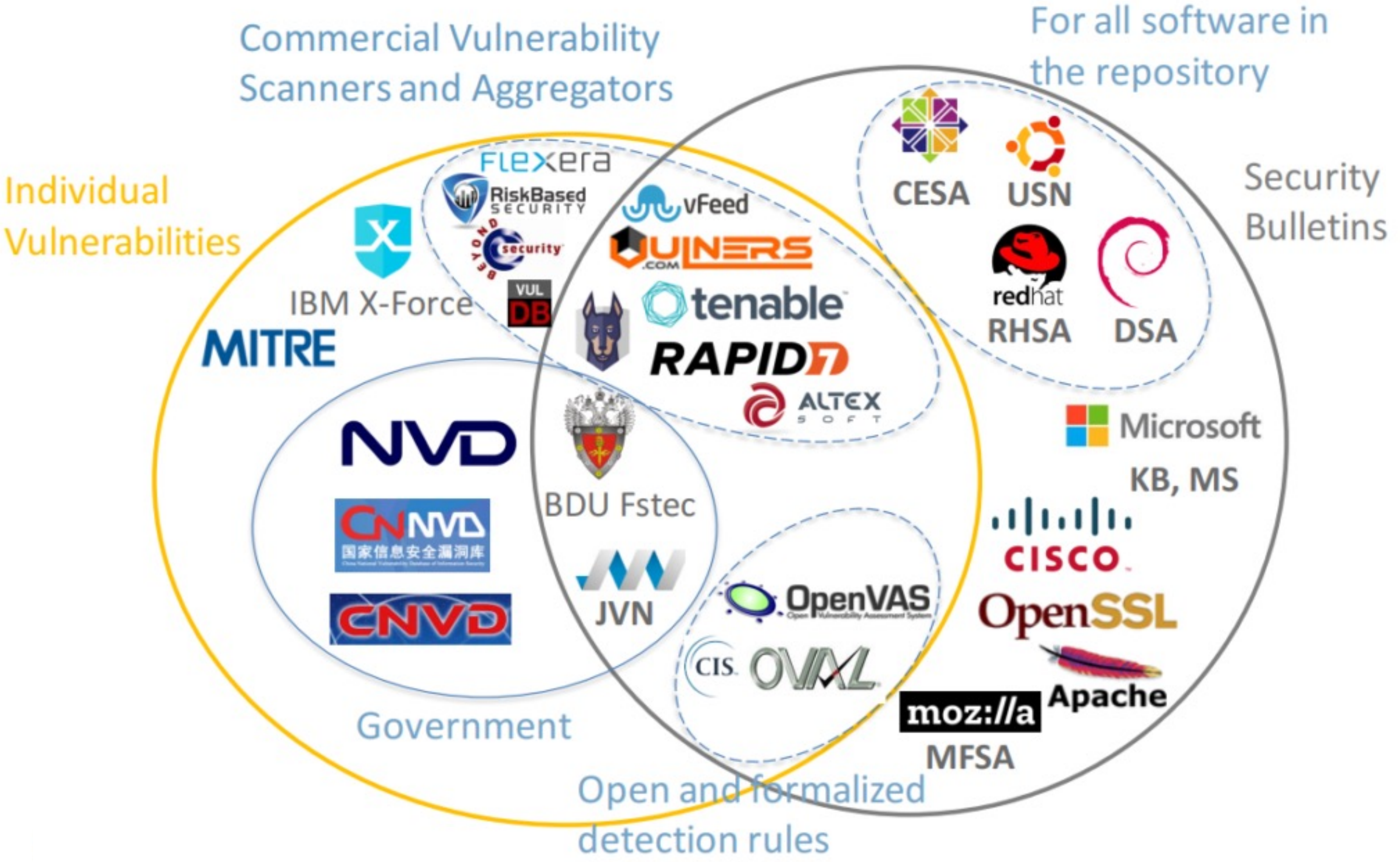
SBOMs & Post-Market Surveillance



```
"type": "library",
"bom-ref": "7fbeec16-6ebb-236f-b486-3023b54f9436",
"name": "FreeRTOS",
"purl": "pkg:supplier/Amazon%20Web%20Services/FreeRTOS@10.3.1",
"publisher": "Amazon Web Services",
"version": "10.3.1"
```



https://avleonov.com/2018/06/05/vulnerability-databases-classification-and-registry/



Commercial Vulnerability Scanners and Aggregators

For all software in the repository

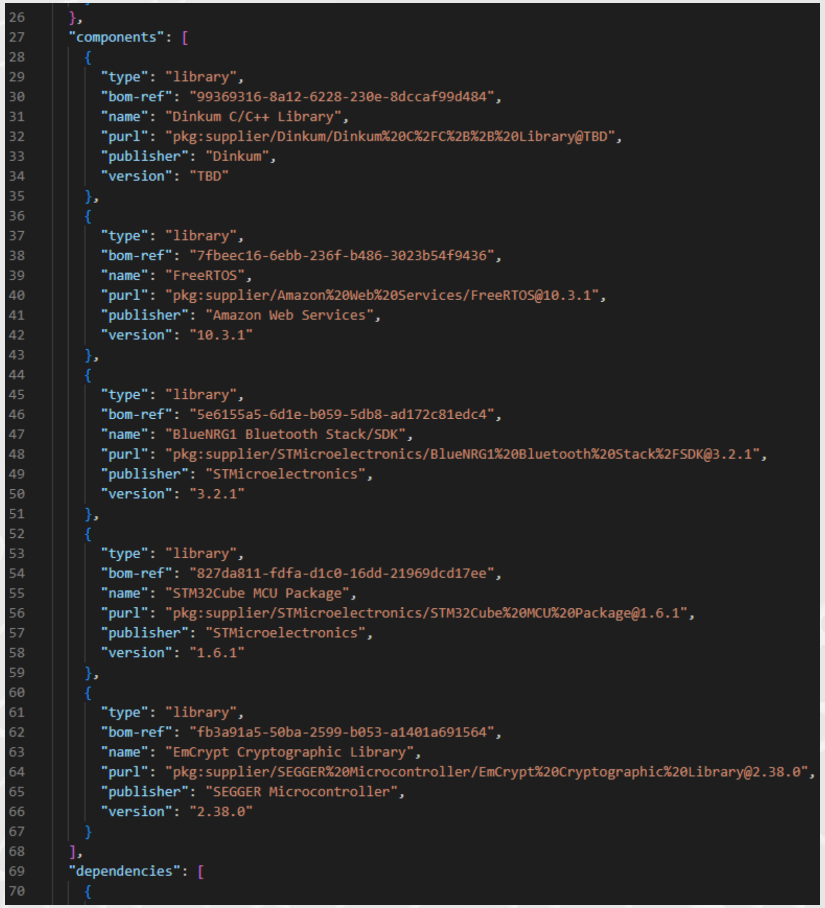
Individual Vulnerabilities

Security Bulletins

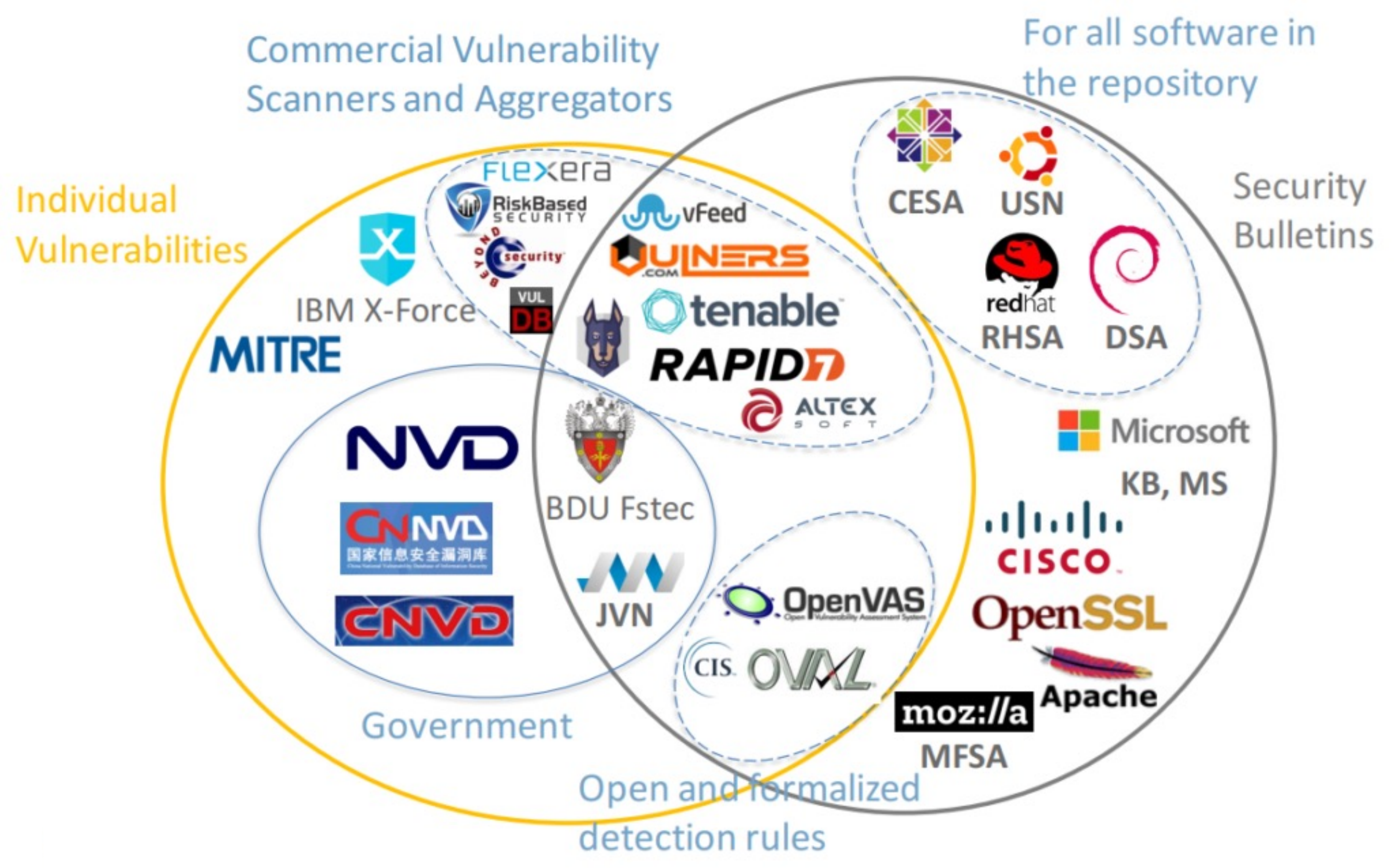
Government

Open and formalized detection rules

SBOMs & Post-Market Surveillance



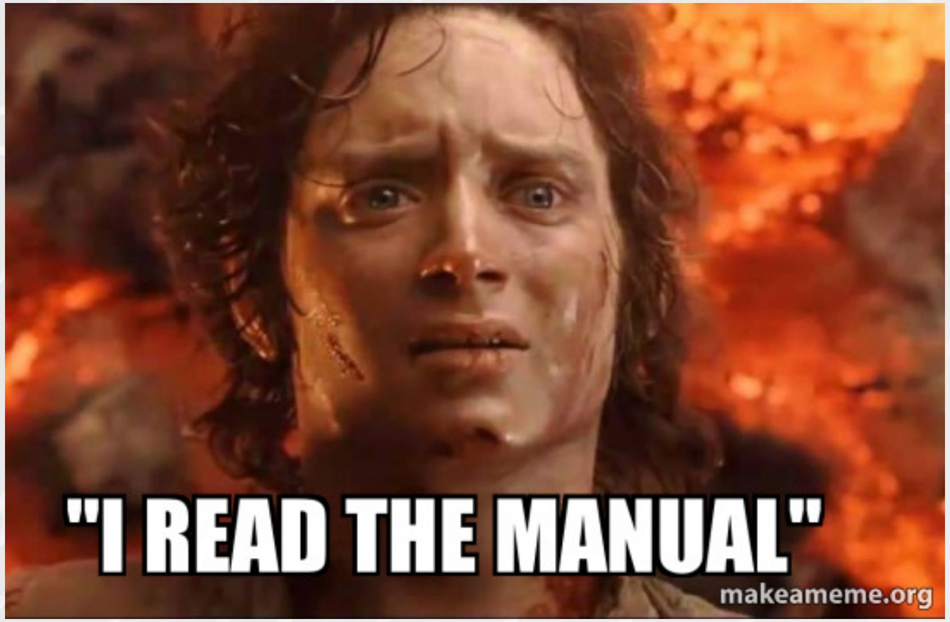
```
  },
  "components": [
    {
      "type": "library",
      "bom-ref": "99369316-8a12-6228-230e-8dccaf99d484",
      "name": "Dinkum C/C++ Library",
      "purl": "pkg:supplier/Dinkum/Dinkum%20C%2FC%2B%2B%20Library@TBD",
      "publisher": "Dinkum",
      "version": "TBD"
    },
    {
      "type": "library",
      "bom-ref": "7fbeec16-6ebb-236f-b486-3023b54f9436",
      "name": "FreeRTOS",
      "purl": "pkg:supplier/Amazon%20Web%20Services/FreeRTOS@10.3.1",
      "publisher": "Amazon Web Services",
      "version": "10.3.1"
    },
    {
      "type": "library",
      "bom-ref": "5e6155a5-6d1e-b059-5db8-ad172c81edc4",
      "name": "BlueNRG1 Bluetooth Stack/SDK",
      "purl": "pkg:supplier/STMicroelectronics/BlueNRG1%20Bluetooth%20Stack%2FSDK@3.2.1",
      "publisher": "STMicroelectronics",
      "version": "3.2.1"
    },
    {
      "type": "library",
      "bom-ref": "827da811-fdfa-d1c0-16dd-21969dcd17ee",
      "name": "STM32Cube MCU Package",
      "purl": "pkg:supplier/STMicroelectronics/STM32Cube%20MCU%20Package@1.6.1",
      "publisher": "STMicroelectronics",
      "version": "1.6.1"
    },
    {
      "type": "library",
      "bom-ref": "fb3a91a5-50ba-2599-b053-a1401a691564",
      "name": "EmCrypt Cryptographic Library",
      "purl": "pkg:supplier/SEGGER%20Microcontroller/EmCrypt%20Cryptographic%20Library@2.38.0",
      "publisher": "SEGGER Microcontroller",
      "version": "2.38.0"
    }
  ],
  "dependencies": [
    {
```



https://avleonov.com/2018/06/05/vulnerability-databases-classification-and-registry/

VI. Labeling Recommendations for Devices with Cybersecurity Risks

- Instructions and product specifications
- Features that protect critical functionality
- Backup and restore info
- Guidance for supporting infrastructure
- Device hardening
- Software update info
- End-of-support info
- Communication interfaces and networking info
- Security event notifications
- Forensic evidence capture (secure logging)
- Diagrams
- SBOM



Medical Device Engineering: Your IP. Designed and Built.