U.S. FOOD & DRUG ADMINISTRATION

Medical Device Cybersecurity

Linda Ricci, MME MPH

Director, Division of All Hazard Response,
Science and Strategic Partnerships

FDA/CDRH/OST

Linda.Ricci@fda.hhs.gov

July 20, 2022

Cybersecurity Flaws Lead to Unavailability

Healthcare Vendor Ransomware Attack Stalls Cancer Treatments, 170 Health Systems Hit

On April 20, 2021, Elekta, a cancer software provider, was targeted by a healthcare ransomware attack. Through the attack, hackers were able to access Elekta's cloud-based software, used t operate radiology equipment. As a result of the incident, Elekta temporarily took their softwa offline, preventing treatment for cancer patients across 170 U.S. health systems. More detail healthcare vendor ransomware attack are discussed.

The New York Times

Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business

All of JBS's beef plants in the U.S. were shuttered on Tuesday, affected, according yees.

The San Diego Union-Tribune

New Perspective on Your Community $4/4 weeks

Scripps ransomware shutdown hits the two-week mark

Scripps

Scripps.org will be back soon

The Scripps Health website is currently unavailable due to a network outage. Patients or families with questions should contact 1-800-SCRIPPS (800-727-4777). We apologize for any inconvenience.

Elekta and DiaSorin were hit with OLD ransomware! Meanwhile, the threats are getting more sophisticated.

TECH

Secret World of Pro-Russia Hacking Group Exposed in Leak

A Ukrainian researcher revealed the operations of Trickbot, one of the

In a secret chat room run by a group of Russian-affiliated cybercriminals, a hacker expressed excitement about a plan to attack and disable more than 400 U.S. hospitals. "There will be panic," the hacker wrote, in Russian.

It was 2020, at a severe point in the pandemic, and the gang planned to hold hostage the computer systems of the hospitals, many of which were fighting to save Covid-19 patients.

WSJ, March 28, 2022 by Robert McMillan, Kevin Poulsen, Dustin Volz

!

U.S. FOOD & DRUG ADMINISTRATION

FDA has prevented devices coming to market

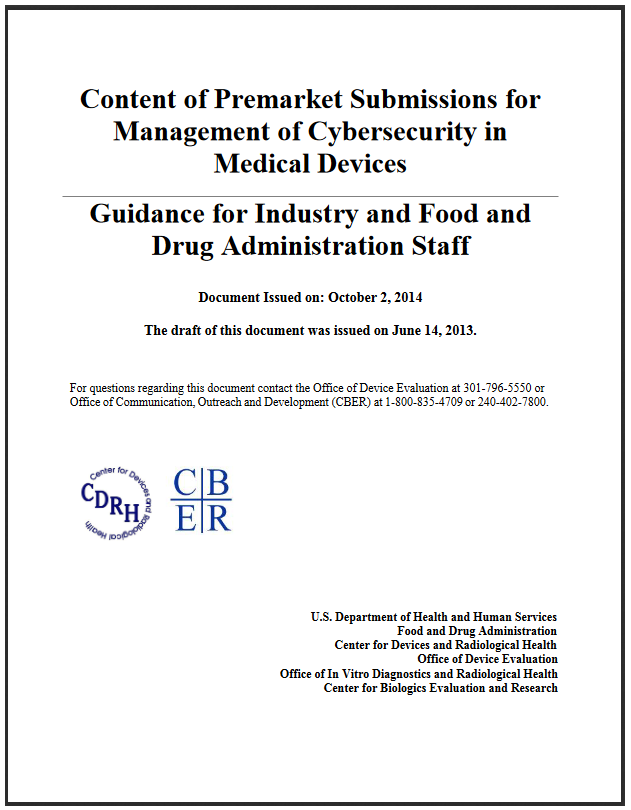
based on cybersecurity concerns alone.

Linda Ricci MME MPH, Director DARSS, FDA CDRH/OST July 2022

Because Cybersecurity is Safety

Linda Ricci MME MPH, Director DARSS, FDA CDRH/OST July 2022

Cybersecurity Guidance: Pre-Market & Post-Market



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

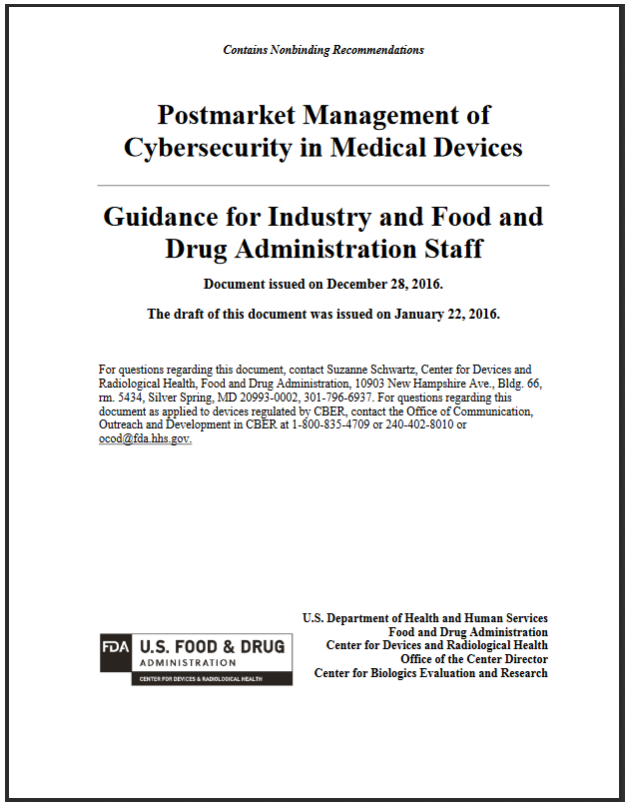
Document Issued on: October 2, 2014

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

2014 finalized pre-market



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

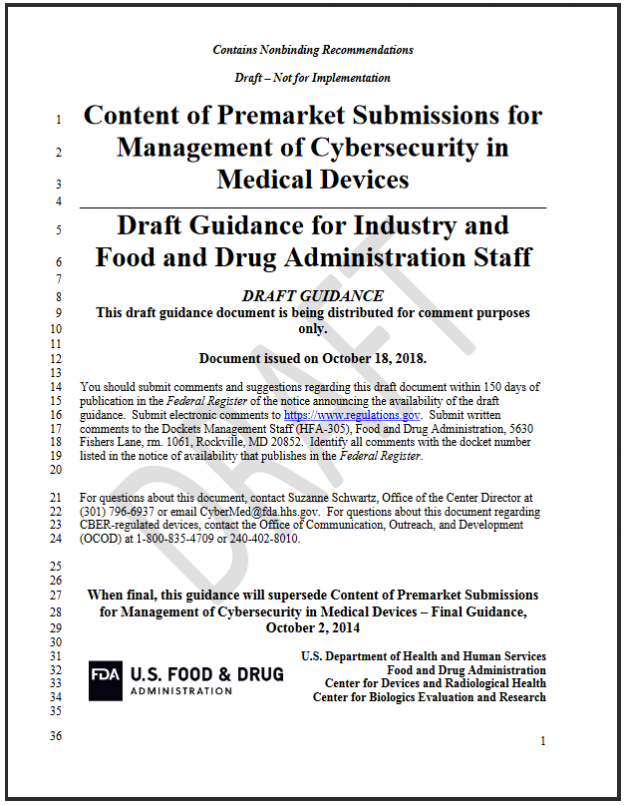
Document issued on December 28, 2016.

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

2016 finalized post-market



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

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

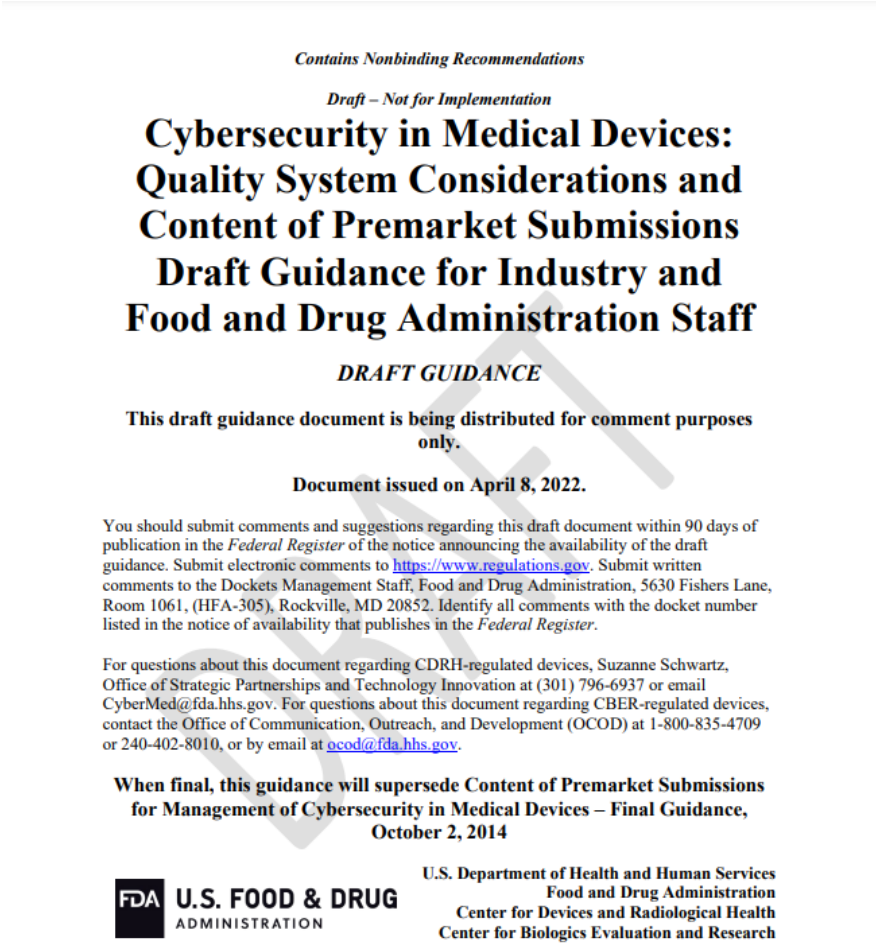
2018 draft pre-market

Revised draft pre-market guidance released for public comment April 2022

2022 revised draft pre-market

2022 Draft Cybersecurity Guidance

- Revised draft premarket medical device cybersecurity guidance published April 7
- Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions
- 90-Day comment period closed July 7, 2022
- Changes from 2018 draft guidance
  - More **detailed technical recommendations** on premarket documentation for cyber risk
  - **Removed risk tiers**; recommends that documentation scale with cyber risk
  - Detailed recommendations on Software Bill of Materials (**SBOM**) and alignment with EO 14028



Contains Nonbinding Recommendations

Draft – Not for Implementation

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions 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 April 8, 2022.

You should submit comments and suggestions regarding this draft document within 90 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, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), 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 regarding CDRH-regulated devices, Suzanne Schwartz, Office of Strategic Partnerships and Technology Innovation 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, or by email at ocod@fda.hhs.gov.

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

A-19 Legislative Activities for Device Security

- Currently **no statutory requirement** expressly requires medical device manufacturers to address cybersecurity
- Draft A-19 establishes **explicit cybersecurity requirements**
  - Software Bill of Materials (SBOM) to track 3rd party risk of software cybersecurity vulnerabilities; a software ingredient list
  - Devices have the capability to be updated and patched in a timely manner
  - Demonstrate reasonable assurance of the device's safety and effectiveness for purposes of cybersecurity
  - Coordinated vulnerability disclosure policy for public disclosure when a manufacturer learns of a cybersecurity vulnerability within a medical device

CDRH Medical Device Cybersecurity Highlights

1. Operational Technology (OT) cybersecurity risks are growing
   - Supply chain risk extends beyond CDRH medical device domain

2. OT cybersecurity is an inherently shared responsibility
   - Necessitates coordination across state + federal government and private sector
   - FDA (CDRH/OST, CDRH/OPEQ, CDRH/Comms), HHS (ASPR, HC3), DHS (CISA), NIST (ITL), private sector, security research firms, patient groups, HDO groups, medical device trade groups, physician societies

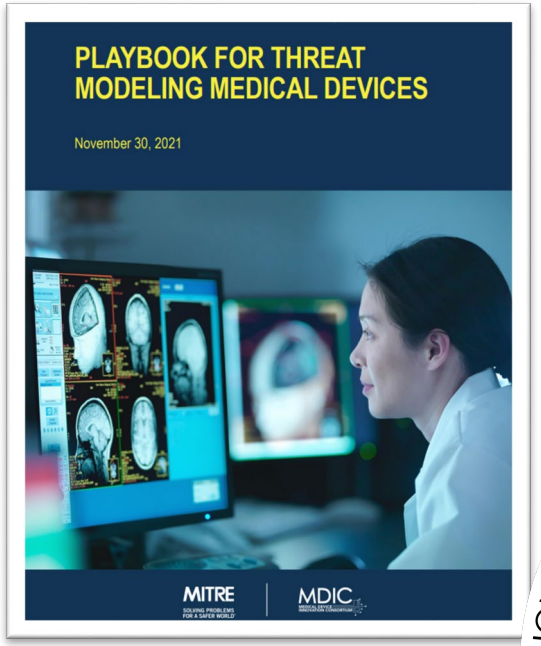
3. CDRH CyberMed team: Total Product Lifecycle (TPLC) approach
   - Pre-market cybersecurity engineering and post-market vulnerability management
   - Provides starting point for agency-wide expertise in OT cybersecurity
   - Digital Health Center of Excellence (DHCoE) designed as a focal point for cross-center cyber coordination

Response to NIST Workshop and Call for Position Papers[1] on Standards and Guidelines to Enhance Software Supply Chain Security[2]

Food & Drug Administration (FDA), Center for Devices and Radiological Health (CDRH) May 26, 2021

Cybersecurity is crucial for medical device safety and effectiveness. Critical functions are shifting from on-premises software infrastructure to distributed and remote infrastructure, including newly essential cloud services depended upon during the diagnosis and treatment of disease. Publicly noted cybersecurity incidents in 2021 include ransomware disabling the Irish Healthcare Service[3], ransomware disrupting a hospital for weeks[4], and a fundamentally new problem where ransomware remediation disrupted the cloud services necessary for critical function of cancer radiation therapy rather than simply disrupting electronic health record systems and other, more traditional hospital IT infrastructure[5]. Such increasingly common ransomware incidents highlight the ungraceful failure of perimeter-based firewalls and the safety consequences of not separating OT from IT by design.

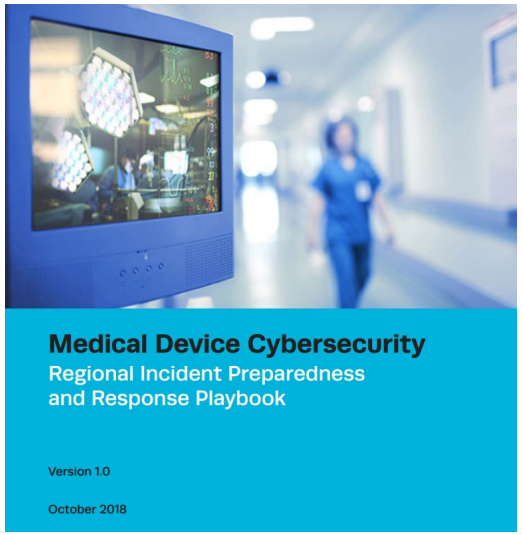
Examples of Ecosystem Resources for Medical Device Cybersecurity



Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN

January 2019



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.