

# Regulatory Affairs: Medical Device Cybersecurity

**Kevin Fu, Ph.D.**

Acting Director, Medical Device Cybersecurity

Program Director for Cybersecurity, Digital Health Center of Excellence (DHCoE)  
FDA/CDRH

*The views expressed herein do not necessarily reflect the official policies of any entity (i.e., businesses, individuals, organizations, institutions or the U.S. federal government, particularly, U.S. Food and Drug Administration (FDA), nor does mention of trade names, commercial practices, or any entity imply an endorsement. FDA is not responsible for the contents of any outside information referenced in this document.*

July 2021



# Kevin's long bio



- Kevin Fu is **Acting Director of Medical Device Cybersecurity at FDA CDRH** and Program Director for Cybersecurity in FDA's Digital Health Center of Excellence (DHCoE). He is **Associate Professor of EECS at the University of Michigan** where he founded the Archimedes Center for Healthcare and Device Security (secure-medicine.org) and directs the Security and Privacy Research Group (SPQR.eecs.umich.edu). He is most known for the original [2008 cybersecurity research paper showing vulnerabilities in an implantable cardiac defibrillator](#) by sending specially crafted radio waves to induce uncontrolled ventricular fibrillation via an unintended wireless control channel. The prescient research led to over a decade of revolutionary improvements at medical device manufacturers, global regulators, and international healthcare safety standards bodies just as ransomware and other malicious software began to disrupt clinical workflow at hospitals worldwide.
- Kevin was recognized as an IEEE Fellow, Sloan Research Fellow, MIT Technology Review TR35 Innovator of the Year, Fed100 Award recipient, and recipient of an IEEE Security and Privacy Test of Time Award. He received the Dr. Dwight E. Harken Lecturer Award from AAMI for his contributions to medical device security. Fu has testified in the U.S. House and Senate on matters of information security and has written commissioned work on trustworthy medical device software for the U.S. National Academy of Medicine. He co-chaired the AAMI cybersecurity working group to create the first FDA-recognized standards to improve the security of medical device manufacturing. He is a founding member of the N95decon.org team for emergency reuse decontamination of N95 masks during PPE shortages. Fu served as a member of the U.S. NIST Information Security and Privacy Advisory Board and federal science advisory groups. Eleven years ago, Fu served as a visiting scientist at the U.S. Food & Drug Administration. Fu received his B.S., M.Eng., and Ph.D. from MIT. He earned a certificate of artisanal bread making from the French Culinary Institute and is an intermediate level salsa dancer.

Ten Years Ago  
to the Day!

FDA



# Medical Devices: Security & Privacy Concerns

**Kevin Fu**

Associate Professor  
Security & Privacy Research Lab  
UMass Amherst Computer Science  
<http://spqr.cs.umass.edu/>  
<http://secure-medicine.org/>



NIST Information Security and Privacy Advisory Board (ISPAB) Meeting  
July 14, 2011

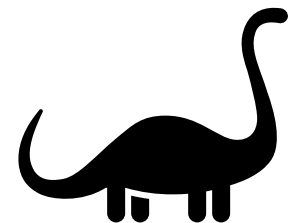
University of Massachusetts Amherst - Department of Computer Science

# Summary: Responsibility is Yours

- Biggest risk:
  - Hackers breaking into medical devices
  - Wide-scale **unavailability** of patient care
  - **Integrity** of medical sensors
- Security can't be bolted on. **Build it in.**
- Cybersecurity responsibility
  - Cybersecurity risks are now considered **foreseeable risks**
  - Design controls in early manufacturing should address risks
  - Update your Windows software!! Don't party like it's 1999.



Regulatory Affairs  
Professionals Society  
(RAPS), Oct 29, 2012





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

# Because Cybersecurity is Safety



# 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

*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](mailto: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

*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.

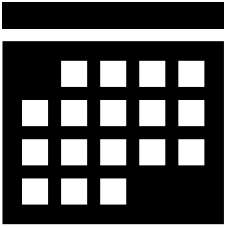
You should submit comments and suggestions regarding this draft document within 150 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to <https://www.regulations.gov>. Submit written comments to the Dockets Management 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](mailto: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



# We are targeting a 2021 Release of the New Draft Premarket Guidance

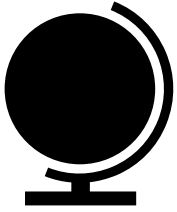


# Threat Modeling



- 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.

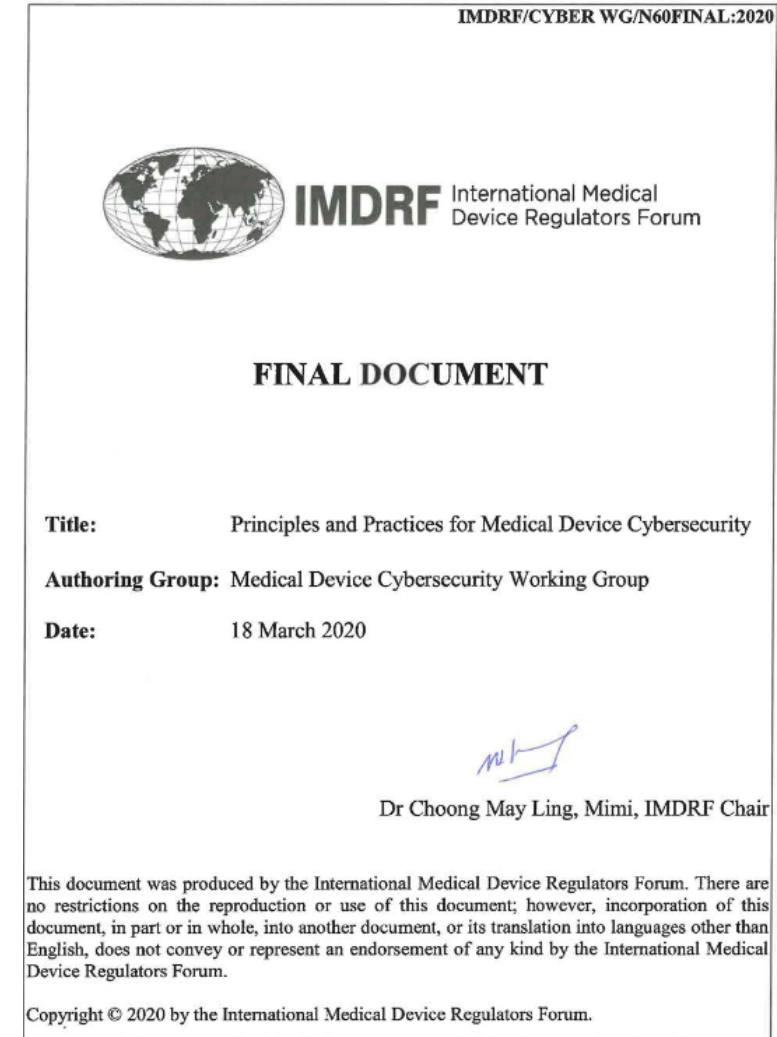




# International Medical Device Regulators Forum (IMDRF)



- 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



# 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

# Joint Security Plan (JSP)



The JSP is a **total product lifecycle reference guide** to developing, deploying and supporting cyber secure technology solutions in the healthcare environment. FDA co-chaired this effort collaboratively with an MDM Lead and HDO Lead as part of the Healthcare and Public Health Sector Coordinating Council (HSCC). Its objective is to establish a voluntary framework and joint security plan for medical devices and healthcare information technology including:

- Cybersecurity practices in design and development of medical technology products
- Handling product complaints relating to cybersecurity incidents and vulnerabilities
- Managing security risk throughout the lifecycle of medical technology
- Assessing the maturity of a product cybersecurity program

**Participants:** Medical Device Manufacturers, Healthcare IT Vendors, Healthcare Providers, Trade Associations, Federal Agencies, Standards Organizations, and Security Technology and Research

**Next Steps:** MDIC cybersecurity maturity benchmarking effort, which seeks MDM participation

<https://healthsectorcouncil.org/the-joint-security-plan/>

# Threat Modeling is Key for 510(k) and PMA Submissions

- Threat Models → Science
  - Identification, analysis, and evaluation of potential security risks (FDA Recognized Consensus Standard AAMI TIR57)
  - Ranks security risks as acceptable, conditionally acceptable, or unacceptable (AAMI TIR57)
  - Avoids “gut judgment” assessments by providing verifiable security design controls (AAMI TIR57)
  - A blueprint to strengthen security through the total product lifecycle of the devices, thereby ensuring improved safety and effectiveness of medical products (MITRE/MDIC Bootcamp)
  - Impossible to make scientific claims of security without a refutable threat model (Kevin Fu)
- Examples of inappropriate (and one appropriate) threat models
  - ~~“We use obscure programming languages”~~ (not science, not refutable)
  - ~~“We’ve never been attacked”~~ (not science, not refutable)
  - ~~“Our product must be placed on a secure hospital network”~~ (networks are inherently hostile)
  - ☺ “We begin by assuming an adversary controls the network with the ability to alter, drop, and replay packets....” (good start)



# NIST Request on Presidential Executive Order: Comments Submitted by the FDA

This report is targeted towards providing relevant responses to the National Institute of Standards and Technology (NIST) call for position papers to fulfill the President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government (EO 14028), issued on May 12, 2021. It highlights existing FDA guidance documents and international standards on the science of cybersecurity for the premarket review of medical device manufacturing and post-market surveillance of cybersecurity incidents and vulnerabilities.

[Download Report \(PDF 4MB\)](#)



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



## **Response to NIST Workshop and Call for Position Papers<sup>1</sup> on Standards and Guidelines to Enhance Software Supply Chain Security<sup>2</sup>**

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<sup>3</sup>, ransomware disrupting a hospital for weeks<sup>4</sup>, 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<sup>5</sup>. 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.



# Cybersecurity Engineering Principles Published by IEEE in 1975



## **The Protection of Information in Computer Systems**

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE

PROCEEDINGS OF THE IEEE, VOL. 63, NO. 9, SEPTEMBER 1975

*Abstract*—This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures—whether hardware or software—that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II



# Cybersecurity Flaws Traceable to Not Following 8 Engineering Principles from IEEE 1975

1. Economy of mechanism: Keep the design as simple and small as possible
2. Fail-safe defaults: Based on permission, not exclusion
3. Complete mediation: Every access checked for authority
4. **Open design principle: Do not depend on ignorance of attackers or security by obscurity**
5. Separation of privilege: Two keys for nuclear launch
6. **(Principle of) Least Privilege (POLP)**
  - **Use least privileges necessary to complete a function (e.g., user vs. root/supervisor)**
7. Least common mechanism: Limit shared resources
  - Unintentionally compromises security. Example: Spectre/meltdown
8. Psychological acceptability: Ease of use of security
  - Users should naturally use and apply protection mechanisms correctly



# Kevin's 2021 Priorities



- Envisioning strategic roadmap for future medical device cybersecurity
- Integrating security principles via CDRH Total Product Life Cycle
- Training/mentoring CDRH staff for pre/post-market reviewing
- Engaging stakeholders in medical device and cybersecurity ecosystem
- Fostering cybersecurity collaborations across federal government
- [Kevin.Fu@fda.hhs.gov](mailto:Kevin.Fu@fda.hhs.gov): External “office hours” Fridays 3-5PM ET

[With thanks to Jessica Wilkerson (Cyber Policy Advisor, FDA CDRH) and Aftin Ross (Senior Science Health Advisor, FD CDRH) for their originally created materials included in these slides ]