FDA CENTER FOR DEVICES &

RADIOLOGICAL HEALTH (CDRH)

PRESENTS A PUBLIC WORKSHOP:

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

January 29-30, 2019

FDA White Oak Campus

Silver Spring, MD

WELCOME

January 29, 2019

Dear Colleagues,

On behalf of the FDA, it is with great enthusiasm that I welcome you to our 2-day public workshop, ***'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices'***.

Advancing and safeguarding the nation's public health warrants attentiveness to the total product life cycle (TPLC) of medical devices, from design to obsolescence. FDA has leveraged this holistic view in its approach to medical device cybersecurity. In 2014, we issued final premarket guidance describing factors that manufacturers should consider in the design and development of medical devices to assure cybersecurity, maintain functionality, and reduce potential risk to patients.

To keep apace with the rapidly evolving nature of cyber threats, we've recently updated our guidance so that manufacturers can be in the best position to proactively address cybersecurity when they are designing and developing their devices – helping to protect against different types of cybersecurity risks, from ransomware to potential catastrophic attacks on health systems and/or on multiple patients. The updated guidance released as DRAFT in October 2018 includes new considerations for device design, labeling and documentation that the FDA recommends be included in premarket submissions for medical devices with cybersecurity risk.

As we reflected on the current landscape during guidance drafting sessions, three cornerstone principles emerged that, in turn, have become the themes of this workshop – *trustworthiness*, *transparency* and *resilience*. When established appropriately in the premarket (design/build) phase, they are, in our view, critical anchors to medical device cybersecurity that set the course for stronger security and improved resilience throughout the product's use life.

While this public meeting builds on the foundational work of prior FDA medical device cybersecurity workshops showcasing collaborative efforts, discussing standards and risk assessment tools and engaging the multi-stakeholder community in focused dialogue on unresolved gaps and challenges, we are especially interested in seeking your input on novel concepts introduced in the guidance. These include: tiering of cybersecurity risk; cybersecurity bill of materials (CBOM); threat modeling and designing for increased resilience, since even with the most robust 'built in' protections, incidents and exploits cannot be entirely eliminated.

We express overwhelming appreciation to all that made this public meeting possible. Much gratitude goes to FDA's Center for Devices and Radiological Health Cybersecurity Working Group, the Emergency Preparedness/Operations & Medical Countermeasures Program, Office of Communications and Education staff, and Center Science Council staff. Planning, organizing and executing a meeting of this size and magnitude is a massive undertaking and today's workshop would not have occurred without their herculean efforts. We would also like to recognize our speakers, moderators, panelists, and facilitators for taking time out of their hectic schedules to partner with us in strengthening cybersecurity within the healthcare and public health sector.

Today we are seeing early fruits of our collective labor, achieved through a "whole of community" approach, and we look forward to your ongoing participation. We may approach cybersecurity from different vantage points, but we all have one common goal and that is to protect patients.

Sincerely,
Suzanne B. Schwartz, MD, MBA

Workshop Themes:

Trustworthiness, Transparency, and Resilience

Workshop Objectives

1. Catalyze critical discussion to help inform finalization of the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices guidance.

2. Foster dialogue on cross-stakeholder efforts to address current and emerging medical device cybersecurity gaps and challenges.

3. Spur collaborations to enable trustworthiness, transparency, and resilience in medical device cybersecurity.

4. Examine considerations for integrating principles of threat modeling and cyber safety into the design of resilient medical devices.

5. Facilitate discussion on Cybersecurity Bill of Materials.

FDA Disclaimer

The views expressed in this Public Workshop are those of the authors and do not necessarily reflect the official policy or position of the U.S. Food and Drug Administration, the Department of Health and Human Services, or the United States Government, and should not be used for advertising or product endorsement purposes. Reference to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its approval, endorsement, recommendation, or favoring by the United States Government or any department, agency, office, or branch thereof.

Contents

Contents

Agenda at a Glance

Agenda Day 1: January 29, 2019	
Time	**Topic**
8:30am-9:00am	Registration (for pre-registered attendees)
9:00am-9:25am	FDA Welcome/Medical Device Cybersecurity State of the Union: Trustworthiness, Transparency and Resilience – A Recipe for Advancing Device Cyber Safety
9:25am-9:30am	Meeting Logistics
9:30am-9:40am	FDA Leadership Remarks
9:40am-9:50am	**BREAK**
9:50am-10:35am	Session I Plenary Panel - Legacy Learnings: Drag of the Past Driving Increased Resilience in the Future
10:35am- 10:50am	Medical Device Premarket Guidance Draft Overview
10:50am-11:35am	Session II Plenary Panel - Threat Modeling & Systems Approaches
11:35am-12:20pm	Session III Plenary Panel - Risk Assessment Approaches & Labeling
12:20pm-1:05pm	**LUNCH**
1:05pm-1:25pm	Keynote
1:25pm-2:05pm	Session IV Plenary Panel - Transitioning from Implied Trust to Trustworthiness: Authentication, Authorization, and Encryption
2:05pm 2:10pm	**Move to Breakout**
2:10pm-2:55pm	Breakout Session: Premarket Guidance Topics Other than CBOM
2:55pm-3:00pm	**Return from Breakout**
3:00pm-3:45pm	Session V Plenary Panel - Increasing Transparency, Advancing Protection, and Enabling Timely Response: Cybersecurity Bill of Materials (CBOM)
3:45pm-3:55pm	**BREAK**
3:55pm-4:45pm	Breakout Session: CBOM
4:45pm	Adjourn

Agenda Day 2: January 30, 2019	
8:30am-9:00am	Registration (for pre-registered attendees)
9:00am-9:30am	Welcome, Day 1 Breakout Report Outs, Recap Day 1
9:30am-10:00am	Session VI Plenary Panel - Patient Perspectives: The True Endpoint
10:00am-11am	Session VII Plenary Panel - Leveraging Innovation and Collaboration to Advance Cyber Safety
11am-11:10am	**BREAK**
11:10am-11:55am	Session VIII Plenary Panel - Scoring Vulnerabilities: What's the clinical context?
11:55am-12pm	**CyberMed Safety (Expert) Analysis Board (CYMSAB) Breakout Framing**
12pm-12:05pm	**Move to Breakout**
12:05pm-12:55pm	Break Out Session: CYMSAB
12:55pm-1:40pm	**LUNCH**
1:40pm-2:40pm	Session IX Plenary Panel - Establishing Trust, Embracing Transparency, Increasing Resilience: Best Practices & Tools
2:40pm-3:25pm	Session X Plenary Panel - Information Sharing: An Evolving Journey
3:25pm-3:35pm	**BREAK**
3:35pm-4:20pm	Session XI Plenary Panel - Preparedness and Response: Wanna Cry Again?
4:20pm-4:40pm	CYMSAB Breakout Report Out, Workshop Recap, and Closing Remarks

Cybersecurity Public Workshop Session Descriptions, Objectives and Questions for Consideration

Day 1

FDA Welcome/Medical Device Cybersecurity State of the Union: Trustworthiness, Transparency and Resilience – A Recipe for Advancing Device Cyber Safety (9:00am- 9:25am)

Suzanne Schwartz, MD, MBA

Associate Director for Science and Strategic Partnerships, Center for Devices and Radiological Health (CDRH) Food and Drug Administration

FDA Leadership Remarks (9:30am-9:40am)

Scott Gottlieb, MD (invited)

Commissioner, Food and Drug Administration

BREAK (9:40am-9:50am)

Session I Plenary Panel (9:50am-10:35am) **– Legacy Learnings: Drag of the Past Driving Increased Resilience in the Future**

Moderator: Zach Hornberger – Medical Imaging and Technology Alliance (MITA)

Session Discussants:

Jennings Aske, JD, CISSP, CIPP/US – New York Presbyterian Hospital

Seth Carmody, PhD – OCD/CDRH / FDA

Julian Goldman, MD – Partners HealthCare & Medical Device Interoperability Program

Jim Jacobson – Siemens Healthineers

Kevin McDonald, BSN, MEPD, CISSP – Mayo Clinic

Michael McNeil – Royal Philips

Colin Morgan, CISSP, GPEN – Johnson & Johnson

Alain Silk, PhD – OIR/CDRH/FDA

Beau Woods – I Am The Cavalry

Session I Objectives:

1. Describe what is meant by the term legacy for the context of this panel
2. Provide a brief overview of some of the cybersecurity legacy challenges
3. Discuss how stakeholders can address safety concerns associated with insecure legacy devices

4. Discuss how we can use learnings from legacy challenges to inform medical device security by design and development going forward

Questions for Consideration:

1. What are some of the cybersecurity challenges associated with legacy devices (e.g. patchability, updatability, device end of life)?
2. What are stakeholder roles and responsibilities regarding legacy devices?
3. How are device manufacturers thinking about addressing legacy challenges in device design?
4. How might stakeholders undertake vulnerability management with legacy devices?
5. What are the expectations of manufacturers regarding legacy device patching?
6. What might communication regarding legacy devices look like between HPH stakeholders, including information sharing and analysis organizations (ISAOs)?
7. What collaborative efforts are underway to address legacy device challenges?
8. How can we use lessons learned from legacy devices to drive resilience in devices going forward?

Medical Device Premarket Guidance Draft Overview (10:35am-10:50am)

Seth Carmody, PhD

Cybersecurity Program Manager, CDRH, Food and Drug Administration

Session II Plenary Panel (10:50am-11:35am) **– Threat Modeling & Systems Approaches**

Moderator: Seth Carmody, PhD – OCD/CDRH / FDA

Session Discussants:

Joe Chapman – MITRE Corporation

Steve Christey Coley – MITRE Corporation

Brian Fitzgerald – OSEL/CDRH/FDA

Billy Rios – QED Secure Solutions

Rob Suarez, HCISPP – Becton Dickinson (BD)

Jason Tugman, CISSP, CRISC, CCSK, ITPM – Axio

Eugene Vasserman, PhD – Kansas State University

Session II Objectives:

1. Describe the criticality of threat modeling as a tool to identify risk and mitigate vulnerabilities throughout the total product life cycle (TPLC)
2. Discuss the limitations and future applications of threat modeling

3. Discuss the difference between compensating and design controls

Questions for Consideration:

1. How does threat modeling inform manufacturers throughout TPLC?
2. What are some of the limitations and assumptions in threat modeling? How do we address these limitations?
3. What is the minimum viable product of threat modeling?
4. Where do you see the future of threat modeling?
5. What are the differences between compensating and design controls?
6. What are the differences between software updates and upgrades?

Session III Plenary Panel (11:35am-12:20pm) **– Risk Assessment Approaches & Labeling**

Moderator: Zach Rothstein, JD – Advanced Medical Technology Association (AdvaMed)

Session Discussants:

Chris Bitza, GSLC, GSIF, GSEC – bioMérieux, Inc

Seth Carmody, PhD – OCD/CDRH / FDA

Christoph Fischer, DIPL.-ING – Roche

Ken Hoyme, MSEE – Boston Scientific

Colin Morgan, CISSP, GPEN – Johnson & Johnson

Dana-Megan Rossi, JD – Becton Dickinson (BD)

Session III Objectives:

1. Describe Tier 1 and Tier 2 devices and rationale for cybersecurity design
2. Discuss needs and expectations regarding design and risk management documentation
3. Discuss needs and expectations for device labeling

Questions for Consideration:

1. How are organizations thinking about integrating risk assessment outputs into new device design?
2. How are organizations thinking about security by design in developing their medical devices?
3. What common errors, omissions, or assumptions are being made regarding risk analysis?
4. What are the challenges and opportunities in taking a systems view to risk analysis (e.g. including components outside of the device such as the manufacturer's network, HDO network, and mobile applications)?
5. How are organizations considering the end user in device labeling?

LUNCH (12:20pm-1:05pm)

Keynote (1:05pm-1:25pm)

Ben Miller, CISSP, GIAC, GREM

Dragos, Inc

Session IV Plenary Panel (1:25pm-2:05pm) **– Transitioning from Implied Trust to Trustworthiness: Authentication, Authorization, and Encryption**

Moderator: Matthew Hazelett – ODE/CDRH/FDA

Session Discussants:

Steve Christie Coley – MITRE Corporation

Joe Chapman, MS – MITRE Corporation

Ken Hoyme, MSEE – Boston Scientific

Tara Larson, CISSP, HCISSP, CSSLP, CISM, CEH – Medtronic

Linda Ricci – ODE/CDRH/FDA

Eugene Vasserman – Kansas State University

Session IV Objectives:

1. Discuss the need to establish trustworthiness of a medical device
2. Discuss the value of taking a systems view in establishing device trustworthiness
3. Describe considerations, approaches, and tools that may be leveraged in the development of a trustworthy device
4. Discuss how the use environment impacts device trustworthiness

Questions for Consideration:

1. Why is it important for medical devices to be trustworthy?
2. What does it mean to take a systems view in establishing the trustworthiness of a device, and what value does it add?
3. How are manufacturers thinking about device authentication and authorization?
4. What approaches and tools may be leveraged in the design of a trustworthy medical device?
5. How does the use environment impact the design and functionality of a trustworthy medical device?
6. What is the difference between authorization from a user versus a device perspective?
7. How might manufacturers communicate the trustworthiness of their device to end users and the FDA?

8. What items, other than device design should be considered to maintain a device's trustworthiness (e.g. key management)?

MOVE TO BREAKOUT (2:05pm-2:10pm)

Breakout Session: Premarket Guidance Topics Other than CBOM (2:10pm-2:55pm)

RETURN FROM BREAKOUT (2:55pm-3:00pm)

Session V Plenary Panel (3pm-3:45pm) **– Increasing Transparency and Enabling Proactive Action: Cybersecurity Bill of Materials (CBOM)**

Moderator: Linda Ricci – ODE/CDRH/FDA

Session Discussants:

Jennings Aske, JD, CISSP, CIPP/US – New York Presbyterian Hospital

Josh Corman – I Am The Cavalry

Zack Hornberger, CISSP – MITA

Jim Jacobson – Siemens Healthineers

Michelle Jump, MS – Nova Leah

Michael McNeil – Royal Philips

Ken Zalevsky – Bayer

Session V Objectives:

1. Discuss what is meant by the term CBOM
2. Discuss the use cases for a CBOM
3. Discuss the type of information that would be of value to include in a CBOM
4. Share the status of current industry efforts (e.g. NTIA Software Transparency, MITA MDS2, etc.)

Questions for Consideration:

1. What cybersecurity challenge(s) does a CBOM seek to address?
2. What are the use cases for a CBOM and what is a CBOM intended to enable?
3. What are the challenges and benefits of including both software and hardware components?
4. What type of information and level of detail that should be included in a CBOM?
5. What are effective mechanisms for sharing CBOM information?

6. What format(s) may be leveraged and what features of a CBOM would make it automatically consumable? Can multiple formats co-exist?
7. What is the appropriate frequency for updating the CBOM?

BREAK (3:45pm-3:55pm)

Breakout Session: CBOM (3:55pm-4:45pm)

ADJOURN (4:45pm)

Day 2

Recap Day 1 (9:00am-9:30am)

Session VI Plenary Panel (9:30am-10am) **– Patient Perspectives: The True Endpoint**

Moderator: Michelle Tarver, MD, PhD – OCD/CDRH / FDA

Session Discussants:

Reid D'Amico, PhD– OCD/CDRH / FDA

Lisa Gilbert, CISSP – Applied Research Systems

Mike Nelson – DigiCert

Jay Radcliffe, CISSP – Thermo Fisher Scientific

Alain Silk, PhD– OIR/CDRH/FDA

Session VI Objectives:

1. Enhance stakeholders' understanding of patient viewpoints regarding medical device cybersecurity

Questions for Consideration:

1. Do you think about the cybersecurity of your device (e.g. are mechanical or digital failures related to cybersecurity)? If you think about the cybersecurity of your device, how does that perspective change (or not) when thinking about the cybersecurity of the device of a loved one such as a child?
2. Would the cybersecurity of your device influence your decision to receive a device or factor into your device choice? If so, how? If not, why not?
3. Have you had any conversations with your doctor about medical device cybersecurity?
4. What role do you think healthcare professionals play in helping patients to consider cybersecurity when making healthcare decisions?
5. What are your expectations of medical device manufacturer communications to patients regarding medical device cybersecurity concerns (e.g. device vulnerabilities)?
6. From a patient's perspective, what would you like FDA to know regarding your thoughts on medical device cybersecurity (cybersecurity features of interest, your risk tolerance, balance between safety and security, etc.)?

Session VII Plenary Panel (10am-11am) **– Leveraging Innovation and Collaboration to Advance Cyber Safety**

Moderator: Beau Woods – I Am The Calvary

Session Discussants:

Denise Anderson, MBA, EMT, NIMS – Healthcare Information Sharing & Analysis Center (H-ISAC)

Daniel Beard – MedISAO

Christian Dameff, MD – University of California, San Diego

Kevin Fu, PhD – Virta Labs & Archimedes Center for Medical Device Security, University of Michigan

Lisa Gilbert, CISSP – Applied Research Systems

Pamela Goldberg, MBA – MDIC

Julian Goldman, MD – Partners HealthCare & Medical Device Interoperability Program

Art Manion – CERT/CC

Nina Alli – DEF CON

Scott Nichols, HCISPP, CHPSE, MCP – Beckman Coulter

Dana-Megan Rossi, JD – Becton Dickinson (BD)

Greg Singleton – HHS

Session VII Objectives:

1. Describe what is meant by coordinated vulnerability disclosure
2. Describe challenges and opportunities to the broad adoption of coordinated vulnerability disclosure (CVD)
3. Understand the roles and responsibilities of various stakeholders in vulnerability disclosure and management
4. Describe the different stakeholder models for vulnerability identification and their value

Questions for Consideration:

1. What is coordinated vulnerability disclosure?
2. What challenges and opportunities impact adoption of CVD?
3. What might help to catalyze the broader adoption of CVD across the medical device industry?
4. What roles do various stakeholders play regarding vulnerability disclosure and management?
5. What vulnerability identification models are stakeholders participating in? (e.g. biohacking village, sandboxes or cyber ranges, simulations)
6. What is the value of participating in these different identification models?
7. What lessons have been learned in establishing and participating in the different vulnerability identification models?

BREAK (11:00AM-11:10AM)

Session VIII Plenary Panel (11:10am-11:55am) **– Scoring Vulnerabilities: What's the Clinical Context?**

Moderator: Phil Englert – Deloitte & Touché

Session Discussants:

Penny Chase, S.M. – MITRE Corporation

Steve Christey Coley – MITRE Corporation

Jim Jacobson – Siemens Healthineers

Art Manion – CERT/CC

Billy Rios – QED Secure Solutions

Jason Tugman, CISSP, CRISC, CCSK, ITPM – Axio

Session VIII Objectives:

1. Raise awareness of various risk assessment scoring systems
2. Describe the challenges that these scoring systems seek to address
3. Identify key characteristics/components of the scoring systems that are needed in the context of the clinical environment

Questions for Consideration:

1. What are some of the available scoring systems and how might they be used?
2. What existing gaps or challenges do these scoring systems address?
3. What are the use cases for your scoring system?
4. What key characteristics and/or components from these scoring systems are needed to assess vulnerability risk in the clinical environment?
5. What challenges remain with the use of these scoring systems?

CyberMed Safety (Expert) Analysis Board (CYMSAB) Breakout Framing (11:55am-12pm)

Margie Zuk, MS

MITRE Corporation

Breakout: CYMSAB (12:05pm-12:55pm)

LUNCH (12:55pm-1:40pm)

Session IX Plenary Panel (1:40pm-2:40pm) **– Establishing Trust, Embracing Transparency, Increasing Resilience: Best Practices & Tools**

Moderator: Greg Garcia – Healthcare Sector Coordinating Council (HSCC)

Session Discussants:

Julia Chua, CISSP – HHS

Erik Decker, MS CISSP – University of Chicago

Anura Fernando, MSE – UL LLC

Brian Fitzgerald – OSEL/CDRH/FDA

Michelle Jump, MS – Nova Leah

Kevin McDonald BSN, MEPD, CISSP – Mayo Clinic

Colin Morgan, CISSP, CISM, GPEN – Johnson & Johnson

Aftin Ross, PhD, MSE – OCD/CDRH/FDA

Rob Suarez, HCISPP – Becton Dickinson (BD)

Ashley Woyak, CISM – Baxter International

Session IX Objectives:

1. Showcase the shared responsibility of healthcare cybersecurity by describing examples of collaborative medical device and healthcare cybersecurity efforts
2. Raise awareness of the tools and resources generated from these collaborations
3. Discuss current cybersecurity standards and those in development
4. Discuss cybersecurity certification schemes for medical devices and/or hospital networks
5. Share lessons learned from medical device cybersecurity collaborations and standards efforts
6. Discuss global considerations for medical device cybersecurity and emerging efforts

Questions for Consideration:

1. What are some examples of collaborations and standards activities in which various stakeholders been engaged?
2. What gap(s) do these collaborations and standards activities address?
3. What challenges have been encountered?
4. What's next for these collaboration and standards efforts?
5. What efforts are occurring in a global context and what if any trends are you seeing?

Session X Plenary Panel (2:40pm-3:25pm) **– Information Sharing: An Evolving Journey**

Moderator: Zach Rothstein, JD – Advanced Medical Technology Association (AdvaMed)

Session Discussants:

Denise Anderson, MBA, EMT, NIMS – Healthcare Information Sharing and Analysis Center (H-ISAC)

Daniel Beard – MedISAO

Rebecca Gagliastro, MBA, MS, PMP – Interstate Natural Gas Association (INGAA)

John Gomez – Sensato

Suzanne Schwartz, MD, MBA – OCD/FDA/CDRH

Session X Objectives:

1. Describe FDA's vision and expectations for medical device vulnerability ISAOs
2. Share lessons learned from information sharing in healthcare and other critical infrastructure sectors such as oil and gas
3. Raise awareness of ISAOs supporting medical device vulnerability information sharing
4. Describe services and resources ISAOs provide to their members and to the stakeholder community at large

Questions for Consideration:

1. What are some of the challenges and opportunities in setting up an information sharing entity?
2. Which stakeholder group(s) do your ISAOs serve?
3. What is FDA's vision for the roles that ISAOs play in medical device vulnerability information sharing?
4. What has been your ISAO's role in vulnerability information sharing and what lessons have you learned as a result?
5. What other services or resources do ISAOs offer to their members? To stakeholders in the community at large?

BREAK (3:25pm-3:35pm)

Session XI Plenary Panel (3:25pm-4:10pm) **– Preparedness and Response: Wanna Cry Again?**

Moderator: Margie Zuk, MS - MITRE Corporation

Session Discussants:

Laura Alfredo, JD – Greater New York Hospital Association

Denise Anderson, MBA, EMT, NIMS – Healthcare Information Sharing and Analysis Center (H-ISAC)

Julie Connolly, CISSP – MITRE Corporation

Christian Dameff, MD – University of California, San Diego

Greg Garcia – Health Sector Coordinating Council

John Gomez – Sensato

Nastassia Tamari– Becton Dickinson (BD)

Zach Rothstein, JD – AdvaMed

Chad Waters – ECRI Institute

Ashley Woyak, CISM – Baxter International

Session XI Objectives:

1. Raise awareness of stakeholder collaborations and resources in medical device cybersecurity preparedness and response
2. Describe the gaps and challenges these activities seek to address
3. Discuss the roles and responsibilities of various stakeholders in medical device cybersecurity preparedness and response
4. Discuss opportunities for stakeholder collaboration in medical device cybersecurity preparedness and response (e.g. tabletop exercises)
5. Share lessons learned from medical device cybersecurity preparedness and response

Questions for Consideration:

1. What medical device cybersecurity preparedness and response collaborations and resources exist?
2. What existing gaps or challenges do these collaborations and resources address?
3. What are stakeholders' (including patients) roles and responsibilities?
4. How else might it benefit stakeholders to collaborate regarding the topic of medical device cybersecurity preparedness and response?
5. What lessons have been learned from other preparedness and response initiatives (e.g. state and local)?

CYMSAB Breakout Report Out, Workshop Recap, and Closing Remarks (4:20pm-4:40pm)

Speaker Biographies

Laura M. Alfredo

Senior Vice President, Legal, Regulatory, and Professional Affairs and General Counsel
Greater New York Hospital Association
lalfredo@gnyha.org

As the Senior Vice President of Legal, Regulatory, & Professional Affairs and General Counsel for Greater New York Hospital Association, Laura Alfredo is responsible for a wide variety of areas implicating hospital legal and regulatory compliance. She advocates for GNYHA members before key regulatory and oversight agencies and provides technical assistance to them on Federal, state and local laws and regulations, as well as compliance program development and implementation. She is also responsible for conceiving and presenting educational programming for members on legal and compliance-related topics.

Prior to joining GNYHA, Ms. Alfredo worked as in-house counsel at two hospital systems in New York City, focusing on compliance, privacy and employment law, as well as litigation. Before that, she was in private practice as a litigator. Ms. Alfredo is a graduate of Fordham University School of Law.

Nina Alli

BioHacking Village Project Manager
DEF CON

Nina earned a B.S. in Interdisciplinary Studies with a focus on Behavioral Sciences, Business, and Communications from the New York Institute of Technology. She has completed two Masters degrees, the first from the University of Illinois at Chicago in Biomedical and Health Informatics, the second from The City College of New York in Translational Medicine with a focus on medical devices. She has participated in the New York Academy of Sciences Fellowship, inaugural member of the Digital Medicine Strategic Planning group, and the Project Manager of the Biohacking Village at DEF CON. Nina has spoken at various international conferences about Biohacking, including DIYBio, Citizen Science, and information research collaboration and integration into medicine.

Denise Anderson, MBA, BA, EMT, NIMS

President
Information Sharing and Analysis Center
H-ISAC

Denise Anderson has over 25 years of executive management level experience in the private sector and is President of the Health Information Sharing and Denise Anderson, MBA, is President of the Health Information Sharing and Analysis Center (H-ISAC), a non-profit organization dedicated to protecting the health sector from physical and cyber attacks and incidents through dissemination of trusted and timely information.

Denise currently serves as Chair of the National Council of ISACs and participates in a number of industry groups and initiatives. In addition, she has served on the Board and as Officer and President of an international credit association, and has spoken at events all over the globe.
Denise was certified as an EMT (B), and Firefighter I/II and Instructor I/II in the state of Virginia for twenty years and was an Adjunct Instructor at the Fire and Rescue Academy in Fairfax County, Virginia for ten years.

She is a graduate of the Executive Leaders Program at the Naval Postgraduate School Center for Homeland Defense and Security.
Denise holds a BA in English, *magna cum laude*, from Loyola Marymount University and an MBA in International Business from American University. She is a graduate of the Executive Leaders Program at the Naval Postgraduate School Center for Homeland Defense and Security.

Jennings R. Aske, JD, CISSP, CIPP/US

SVP, Chief information Security Officer
NewYork-Presbyterian Hospital
jraske@nyp.org

Jennings Aske is a Senior Vice President and the Chief Information Security Officer for NewYork-Presbyterian Hospital. Previously, Jennings was the Chief Information Security and Privacy Officer of Partners HealthCare System. Jennings also has served as the Chief Information Security Officer for Nuance Communications, UMass Memorial Hospital, and the Commonwealth of Massachusetts's Executive Office of Health and Human Services. Jennings is a licensed attorney in the Commonwealth of Massachusetts. Jennings graduated from Boston University Law School in 2002, where he was a member of the American Journal of Law & Medicine.

Daniel Beard

Director, MedISAO
CTO, Promenade Software
daniel@medisao.com

Daniel is the founder and director of MedISAO, the first Information Sharing and Analysis Organizations created specifically for Medical Device manufacturers. Through actively analyzing and sharing cyber threats MedISAO helps Medical Device companies stay on top of their product's cybersecurity. By providing training and tools such as Software Bill of Materials (SBOM) generation and Coordinated Vulnerability Disclosure, MedISAO greatly enhances secure product design.

In addition to managing MedISAO Daniel is a founder and CTO of Promenade Software, Inc. Promenade specializes in developing software, including mobile and cloud solutions, specifically, for Medical Device Manufacturers. He has more than a decade of experience building software and advising Medical Device companies how to keep their devices secure.

Daniel presents on the topic of cybersecurity at several Medical Device conferences including BSides, DEF CON, DeviceTalks and OCRA. He enjoys volunteering with several cybersecurity groups that focus on information sharing and software transparency.

Daniel has a BS in Computer science from the University of California, Irvine.

Chris Bitza, GSLC, GSIF, GSEC

US Product Cybersecurity Leader
bioMérieux, Inc
chris.bitza@biomerieux.com

Chris has spent the last 23 years in the design, testing, and delivery of complex software systems in the fields of banking, agriculture bio-tech, pharmacy management, and healthcare delivery. For the past 12 years he has worked within the R&D Systems Development team at bioMerieux, Inc, leading global teams of Business & Systems Analysts and Software Verification Testers. He has served as the US Commercial Product Security Lead since 2014. Working in close collaboration with his French counterpart, he has planned and implemented bioMérieux's Product Security Program, Secure Development Lifecycle, Patch Management program, Vulnerability Management program, and established product improvement roadmaps for all US based products. bioMérieux is an international company with subsidiaries in 42 nations. Chris works closely with bioMérieux's Global Regulatory team to ensure all relevant security regulations standards and guidances have been considered in the design of bioMérieux's Security Program, and advises the Standards Watch Committee on all emerging international security standards. He provides guidance to the Import/Export Compliance Officer on matters relating to security and encryption technology, and partners with the Chief Privacy Officer to ensure all global privacy regulations are respected during system's design and development.

Chris has spoken at the Archimedes Leadership conference and recently co-chaired the 2019 Archimedes 101 Conference. As a member of the Calvary he volunteers at the DEFCon bioHacking Village to share the complexities of healthcare and medical device security with the research community. Father of two, fan of family board games, lover of tacos, craft beer hunter, Cubmaster.

Seth D. Carmody, Ph.D.

Cybersecurity Program Manager
Office of the Center Director
US FDA
seth.carmody@fda.hhs.gov

Dr. Carmody is the Cybersecurity Program Manager for the Center for Devices and Radiological Health, serving as co-chair of CDRH's Cybersecurity Working Group. The Cybersecurity Working Group is an interdisciplinary team responsible for the CDRH's cybersecurity guidances and incident response. Seth joined CDRH in 2011 as a medical device reviewer.

Joseph Chapman, MS

Principal Hardware Security Engineer
The MITRE Corporation
jchapman@mitre.org

Joseph Chapman received his B.S. degree in electrical and computer engineering from Worcester Polytechnic Institute, Massachusetts, in 2005 and his M.S. degree in electrical engineering with a concentration in signal processing and communication systems from Northeastern University, Boston, Massachusetts, in 2014. He is a principal hardware security engineer and group leader at the MITRE Corporation in Bedford, Massachusetts. His group's research focuses on hardware security topics, including cryptographic implementations, fault and side-channel attacks and countermeasures, secure design practices and architectures, and cyber-physical and legacy system security.

Penny Chase, S.M.

Information Technology and Cybersecurity Integrator
The MITRE Corporation
pc@mitre.org

Penny Chase is the Information Technology and Cyber Security Integrator in the Information Technology Technical Center at The MITRE Corporation. She has led MITRE and government-sponsored projects in sharing healthcare fraud data, applying natural language processing to medical device adverse event reports, developing structured representations for malware and threat information, security visualization, software assurance, malware analysis, reverse engineering, software architecture and design pattern recovery, network penetration testing, legacy database encapsulation, machine learning, and discourse-based natural language interfaces. Penny currently supports MITRE's FDA/CDRH projects on medical device cybersecurity (leading the effort to develop a Common Vulnerability Scoring System rubric tailored to medical devices) and cyber security preparedness and response, and MITRE's cyber security coordination activities for the DoD/VA Interagency Program Office. Previously she led the Malware Attribute Enumeration Characterization (MAEC) project for DHS; served as the Deputy Director of the ARDA Northeast Regional Research Center, managing workshops that addressed Intelligence Community challenge problems; and was a member of the NASA Advisory Council's subcommittee on Avionics, Software, and Cybersecurity.

Penny earned a B.A. in History and Mathematics from Binghamton University, and then received an A.M. in the History of Science and an S.M. in Computer Science from Harvard University.

Steve Christey Coley

Principal INFOSEC Engineer
Trust & Assurance Cyber Tech Department
The MITRE Corporation
coley@mitre.org

Steve Christey Coley is a Principal Information Security Engineer in the Cyber Security Division at The MITRE Corporation, supporting the FDA CDRH on medical device cyber security, including coordinated vulnerability handling and disclosure, risk assessment, and methods of applying CVSS to healthcare. He is the technical lead for the Common Weakness Enumeration (CWE).

With cybersecurity experience dating back to 1993, Steve was the co-creator and Editor of the Common Vulnerabilities and Exposures (CVE) list and chair of the CVE Editorial Board from 1999 to 2015, and the technical lead for the Common Weakness Scoring System (CWSS) and the community-driven CWE/SANS Top 25 Software Most Dangerous Software Errors lists from 2009 to 2011. He was a co-author of the "Responsible Vulnerability Disclosure Process" IETF draft with Chris Wysopal in 2002. He was an active contributor to other efforts, including the Common Vulnerability Scoring System (CVSS) version 2, the Common Vulnerability Reporting Framework (CVRF), NIST's Static Analysis Tool Exposition (SATE), various projects involving the assessment of static code analysis tools, and the SANS Secure Programming exams. His current interests include ensuring that emerging technologies do not repeat the chaotic path to effective vulnerability management that occurred with enterprise IT software in the 1990s; secure software development and testing; consumer-friendly software security metrics; the theoretical underpinnings of vulnerabilities; and making the cybersecurity profession more inclusive, diverse, and accessible to everybody who seeks a place in it. He holds a B.S. in Computer Science with a minor in Sociology from Hobart College.

Julie Chua, PMP, CISSP

Risk Management Branch Chief
HHS Cybersecurity Program/HHS Office of Information Security/OCIO
U.S. Department of Health and Human Services (HHS)
Julie.chua@hhs.gov

Julie joined the Governance, Risk Management and Compliance (GRC) Division within the HHS Office of Information Security (OIS) in October 2015. As the Risk Management Branch Chief, Julie is responsible for establishing a Department-wide enterprise risk management program. Julie also leads high visibility initiatives including the identification and protection of HHS' most critical high value assets and the HHS FedRAMP and Cloud Security Program. Julie is a regular speaker at conferences and at HHS leadership meetings where she briefs executive leadership across all HHS Operating Divisions on upcoming risk management initiatives.

Julie is also the Federal Lead for the implementation of the Cybersecurity Act (CSA) of 2015, Section 405(d): Aligning Healthcare Cybersecurity Approaches. This public-private partnership effort is one of many HHS cybersecurity initiatives to help push forward the cybersecurity and resiliency of the HPH sector.

Prior to joining HHS OIS, Julie served as the Cybersecurity Team Lead within the Office of the National Coordinator for Health IT (ONC) at HHS. In her previous role, Julie was the lead on White House Critical Infrastructure Cybersecurity efforts and spearheaded these initiatives across HHS, its federal partners, and the private sector. She led the effort to establish an information sharing and analysis organization (ISAO) specific for the HPH sector to enable widespread dissemination of cyber threat information, general cybersecurity best practices and lessons learned. Information sharing enhances the ability of the federal government to protect the sensitive personal and health data of millions of Americans. She also initiated the creation of a crosswalk between the HIPAA Security Rule and the NIST Cybersecurity Framework. This crosswalk is now available to HPH sector stakeholders such as hospitals and public healthcare facilities, small and medium-sized providers, providing additional guidance and capabilities towards implementing robust risk management programs.

Before joining the federal government, Julie was a small business owner with projects that focused on federal information security policies, risk assessments, enterprise-level software application development.

Julie Connolly, CISSP

Principal Cybersecurity Engineer
The MITRE Corporation
jconnoll@mitre.org

Julie Connolly, CISSP, is a **Principal Cybersecurity Engineer** with more than 20 years in MITRE's Cyber Solutions Technical Center. She has experience across the cybersecurity domain: policy, strategy, standards, research, and operations. She is part of a MITRE team supporting the U.S. Food and Drug Administration (FDA) effort to engage cross-sector stakeholders and develop a collaborative approach to managing medical device cybersecurity. She is also providing cybersecurity support to the Veteran's Administration (VA). She has helped make governance and cybersecurity recommendations to improve the Department of Health and Human Services' (HHS) IT infrastructure, as well as helped mature the Centers for Medicare and Medicaid Services' (CMS) cyber threat intelligence capability. She has led MITRE's internal Cybersecurity Operations Team, led several internal MITRE cybersecurity research projects, led the Common Malware Enumeration (CME) initiative, participated in the Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) standards development efforts, led vulnerability testing and assessment efforts, and supported the National Information Assurance Program (NIAP).

Julie is a cyber threat–based defense advocate, having seen the benefits firsthand at MITRE. She is working to channel these insights and lessons learned to help the healthcare sector realize the advances made by the defense and finance sectors. Prior to joining MITRE, Julie was a captain in the U.S. Air Force. Julie has a B.S. in Computer Science and Sociology from the University of Michigan.

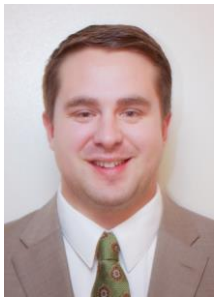
Joshua Corman

Founder of I am the Cavalry and CSO for PTC
joshcorman@gmail.com

Joshua Corman is a Founder of I am The Cavalry (dot org) and CSO for PTC. Corman previously served as Director of the Cyber Statecraft Initiative for the Atlantic Council, CTO for Sonatype, Director of Security Intelligence for Akamai, and in senior research, analyst, & strategy roles. He co-founded RuggedSoftware and IamTheCavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. Josh's unique approach to security in the context of human factors, adversary motivations, and social impact has helped position him as one of the most trusted names in security. He also serves as an adjunct faculty for Carnegie Mellon's Heinz College and served on the Congressional Task Force for Healthcare Industry Cybersecurity.

Christian Dameff, MD

Clinical Informatics Fellow
Department of Emergency Medicine
University of California San Diego
cdameff@ucsd.edu



Dr. Christian Dameff an Emergency Physician, Clinical Informatics Fellow, and researcher. Published clinical works include post cardiac arrest care including hypothermia, novel drug targets for acute myocardial infarction patients, ventricular fibrillation waveform analysis, cardiopulmonary resuscitation (CPR) quality and optimization, dispatch assisted CPR, teletoxicology and medical education topics using Google Glass.

Dr. Dameff is also a hacker and security researcher interested in the intersection of healthcare, patient safety, and cybersecurity. He has spoken at some of the world's most prominent hacker forums including Defcon, RSA, Blackhat, Derbycon, BSides: Las Vegas, and is one of the cofounders of the CyberMed Summit, a novel multidisciplinary conference with emphasis on medical device and infrastructure cybersecurity. Published cybersecurity topics include hacking 911 systems, HL7 messaging vulnerabilities, and malware.

Reid W. D'Amico, Ph.D.

AIMBE Scholar
Office of the Center Director
U.S. FDA
reid.damico@fda.hhs.gov

Dr. D'Amico is an AIMBE Scholar and member of the cybersecuity team for the Center for Devices and Radiological Health. As a medical device user himself, Reid is particularly interested in the intersection of patient persepctives and cybersecuity. Before joining FDA, Reid was a National Science Foundation Graduate Research Fellow at Vanderbilt University until earning his PhD in Biomedical Engineering. His doctoral research focused on designing next generation models of pulmonary vascular disease. Reid is also a rare disease advocate and has worked with pharmaceutical companies to help design clinical trial protocols and increase company-patient engagement. Reid also served as the laboratory instructor for Biomedical Instrumentation and Medical Device Design at Vanderbilt. Reid got his start in medical devices at Duke University, where he graduated *cum laude* with a BSE in Biomedical Engineering.

Erik Decker

Chief Information Security & Privacy Officer
The University of Chicago Medicine
erik.decker@uchospitals.edu

Erik Decker is the Chief Security and Privacy Officer for the University of Chicago Medicine, and is responsible for its Cyber Security, Identity and Access Management and HIPAA Privacy Programs. Erik has 18 years of experience within Information Technology, with 12 years focused on Information Security. The majority of his career has been focused on Academic Medical Centers; establishing two information security programs and an identity and access management program.

Erik is the current Chair of the Association for Executives in Healthcare Information Security (AEHIS) Board. This association focuses on educating over 900 CISOs and providing cybersecurity resources within the Healthcare sector, as well as advocating for Healthcare Information Security needs in both regulatory affairs and legislative affairs capacities.

He is currently Co-Leading a Department of Health and Human Services (HHS) task group of more than 150 industry experts across the country for implementing the CISA 405D legislation within the Healthcare sector. This group is charged with "Aligning the Health Care Industry Security Approaches", as well as implementing several components of the recently federal Cybersecurity Task Force report. He is also a leader of the HHS Joint Cybersecurity Work Group, which is a public-private workgroup formed under the National Infrastructure Protection Plan. He was awarded the 2017 Chicago CISO of the Year in October, 2017. Lastly, he previously served as an adjunct faculty member at Columbia University teaching HIPAA Privacy and Security.

Erik has a Master's of Science in Information Technology from Loyola University in Chicago and Bachelors degree of the University of Illinois in Champaign/Urbana in Cell and Structural Biology.

Phil Englert

Global Clinical Technology Leader
Cyber Risk/Denver
Deloitte & Touché
penglert@deloitte.com

Phil is the Global Clinical Technology Leader at Deloitte with over 30 years' experience in healthcare technology management supporting operations, strategy, and security. Prior to Deloitte, Phil worked as the Vice President of Health Systems at Medical Device Innovation Security and Safety Consortium (MDISS) and at Catholic Health Initiatives (CHI), one of the nation's largest non-profit health systems, for 23 years. At CHI, Phil oversaw medical device IT security, integration, and risk distribution as System Director, Technology Operations. This included developing a methodology for enterprise-wide assessment of medical device IT vulnerabilities, establishing working relationships with CE and IT workstreams, and reducing medical device maintenance costs through self-funded extended warranty programs.

Throughout his career, Phil has provided key leadership in the development and delivery of cooperative and integrated Clinical Engineering, IT Security, Legal, and Corporate Responsibility efforts that enable comprehensive medical device security programs in cyber-hostile environments. He has led multidisciplinary teams to assess and address medical device security, developed operational and quality benchmarking programs, and created and delivered successful life cycle management strategies. Phil received a B.A. from Thomas More College.

Anura Fernando, MSE

Chief Innovation Architect
Medical Systems Interoperability and Security
UL LLC
Anura.S.Fernando@ul.com

Mr. Fernando currently has global responsibility for medical device software certification programs at UL and serves as UL's technical lead for the development of the AAMI/UL 2800 family of standards for interoperable medical device safety and platform security, and the UL 2900-2-1 product-testing focused cybersecurity standard for healthcare. He also represents the U.S. in many international standards development efforts.

He has served on the US Department of Health and Human Services Cybersecurity Task Force, FDA Safety and Innovation Act (FDASIA) working group, FDA Medical Device Interoperability Coordinating Council, Medical Device Interoperability Safety Working Group, IECEE Expert Task Force, NIH QMDI Program Advisory Committee, NIH PRISM Industry Expert Committee, et al. He is a member of the Association for the Advancement of Medical Instrumentation, Health Information Management Systems Society, and the International Council on Systems Engineering.

Mr. Fernando also leads UL's cybersecurity efforts with the VA under the UL-VA Cybersecurity Cooperative Research and Development Agreement.

In addition to holding degrees in Electrical Engineering, Biology/Chemistry, and Software Engineering, Mr. Fernando has over 20 years of experience at UL with safety critical software and control systems certification. His research spans multiple application domains – industrial automation, alternative energy, medical / laboratory, explosive atmospheres, bio-fuels, appliances, optical radiation, nanotechnology, and battery technologies, and includes research publications on predictive modeling and risk analysis, cybersecurity, systems of systems, software, Health IT, apps, wearables, interoperability, and medical device safety.

In addition to his research, Mr. Fernando manages multiple projects for bringing innovative new technologies to the market with numerous Fortune 500 companies as well as start-ups, DoD, DoE, DHS, FDA, FCC, ONC, NASA, and several U.S. National Laboratories.

Christoph Fischer, Dipl.-Ing.

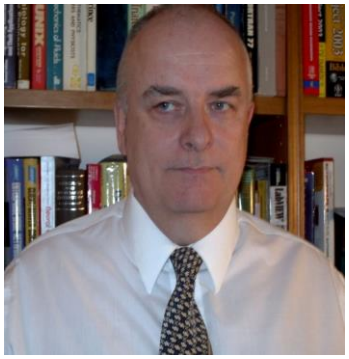
Sr. Systems Engineer Modeling & Design
Co-Chair IEEE 11073 PHD Cybersecurity Working Group
Roche Diabetes Care GmbH
christoph.fischer@ieee.org

From 2005 to 2014, Christoph Fischer worked for Weinmann Medical Technology and participated in the development of pulse oximeters, sleep diagnostic devices, sleep therapy devices, home ventilators and cloud solutions. Since 2014, he works as a Lead System Engineer for Roche Diabetes Care. In the design and life-cycle of a new generation of insulin pumps and diabetes managers, he leads a team responsible for the system definition, system integration, interoperability with third-party solutions and cybersecurity. Christoph Fischer is an active member of the IEEE 11073 PHD Working Group since 2010, the Personal Connected Health Alliance (previously known as Continua) since 2010 and Bluetooth Medical Devices Working Group since 2014 participating in the development of standardized and interoperable data exchange protocols. Currently, Christoph Fischer co-chairs the IEEE 11073 PHD Cybersecurity Working Group efforts on the standardization of secure Plug & Play Interoperability for Personal Health Devices.

Christoph Fischer earned a Dipl.-Ing. degree (equivalent to a Master degree) in Electrical Engineering & Information Technology with a discipline in Biomedical Engineering from the Karlsruhe Institute of Technology in Karlsruhe, Germany in 2005.

Brian J. Fitzgerald

Senior Technical Manager
FDA
brian.fitzgerald@fda.hhs.gov



The last 28 years have been dedicated to the development and implementation of various medical quality assurance related and medical software safety, cybersecurity and assurance programs, based both in the US and overseas. Prior to this, 14 years petro-physical data acquisition, interpretation, and analysis experience in the domestic and international arenas, of which 5 years experience in model/algorithm development, data modeling, customer interfacing, interpretation training, and application software development. Special interests are in the area of medical device software (i.e. safety critical) systems, cybersecurity, business systems (vis-à-vis supplier/purchaser) compliance to ISO 9000, ISO 13485, EN 46000 series (among others), and in the area of data interpretation/acquisition and quality assurance.

Kevin Fu, PhD

Associate Professor,
Archimedes Center for Medical Device Security at the University of Michigan and Chief Scientist, Virta Labs, Inc
kevinfu@umich.edu

Dr. Kevin Fu is credited for establishing the field of medical device security beginning with the 2008 IEEE paper on defibrillator security. Kevin is Chief Scientist of Virta Labs, Inc. and Associate Professor in EECS at the University of Michigan where he directs the Archimedes Center for Medical Device Security and the Security and Privacy Research Group (SPQR) at secure-medicine.org.

Kevin has testified in the House and Senate on matters of information security and has written commissioned work on trustworthy medical device software for the Institute of Medicine of the National Academies. He has briefed White House staff on methods to improve medical device security. Kevin was named MIT Technology Review TR35 Innovator of the Year. Kevin served as program chair of USENIX Security, a member of the NIST Information Security and Privacy Advisory Board, and co-chair of the AAMI Working Group on Medical Device Security. He served as a visiting scientist at the Food & Drug Administration, the Beth Israel Deaconess Medical Center of Harvard Medical School, Microsoft Research, and MIT CSAIL. Kevin received his B.S., M.Eng., and Ph.D. from MIT. He earned a certificate of artisanal bread making from the French Culinary Institute.

Rebecca Gagliostro MBA, MS, PMP

Director of Security, Reliability, and Resilience
Interstate Natural Gas Association of America
rgagliostro@ingaa.org

Rebecca joined the Interstate Natural Gas Association of America in December 2017 and serves as the Director of Security, Reliability, and Resilience. In her role, she leads INGAA's cyber and physical security efforts. Rebecca most recently worked at the American Gas Association, where she supported the cybersecurity, physical security, and underground storage initiatives of AGA's member companies.

Prior to joining AGA, Rebecca was Program Manager for Cybersecurity and Critical Infrastructure at Energetics Incorporated, a management consulting firm specializing in energy and infrastructure resilience. In that role, she supported clients at the U.S. Department of Energy focused on energy sector cybersecurity research and development to enhance the reliability and resilience of the nation's energy infrastructure. Rebecca has a B.S. in Integrated Science and Technology with concentrations in Energy and Environment from James Madison University and Business Administration/Information Technology dual master's degrees from Marymount University.

Gregory T. Garcia

Executive Director for Cybersecurity
Health Sector Coordinating Council

Greg Garcia is the Executive Director for Cybersecurity of the Health Sector Coordinating Council, the convening organization for critical healthcare infrastructure organizations across 6 major subsectors, working in partnership with HHS and other government agencies to protect the security and resilience of the sector, patient safety and public health.

Greg was appointed by President George W. Bush as the nation's first Assistant Secretary for Cybersecurity and Communications with the U.S. Department of Homeland Security. One of his major achievements in this role was conceiving and initiating creation of the National Cyber and Communications Integration Center, the nation’s 24x7 public-private partnership for cybersecurity watch, warning, analysis and incident response.

He also served as executive director of the Financial Services Sector Coordinating Council, and held senior executive positions with Bank of America, 3Com Corporation, Information Technology Association of America, and American Electronics Association, all with the responsibility of driving change in public policy and business operations to strengthen the security and resiliency of the nation's critical infrastructures.

Greg served as a professional staff member on the Committee on Science in the U.S. House of Representatives, where he helped draft and shepherd enactment of the Cyber Security Research and Development Act of 2002.

Greg serves on the Information Security and Privacy Advisory Board, a government/industry committee advising the Secretaries of Commerce and Homeland Security, and the Director of OMB, on national information security and privacy policy.

Lisa Gilbert, CISSP

Cybersecurity Instructor
Air Force Cybersecurity Control Weapon System Forward Training Unit
Applied Research Solutions
lisa@cybersecuritystudio.com

Lisa Gilbert is a cybersecurity instructor with Applied Research Solutions for the Cybersecurity Control Weapon System Forward Training Unit of the Air Force. She specializes in Attack and Defense Strategies, Vulnerability Assessment and Remediation, and Client Endpoint Protection. As an intern with a small cybersecurity company, she created HIPAA training curriculum for medical staff. She has created a website (www.cybersecuritystudio.com) to provide study aids for her students pursuing Security+ and CISSP certifications, and also writes a blog for laypeople to assist in understanding cybersecurity issues that affect them. She previously worked for Honeywell Aerospace, where she designed and implemented real-time, embedded guidance software for commercial aircraft, as part of the team that developed the first commercial polar guidance software. She was technical lead for lateral guidance, navigation, and the electronic flight instrumentation system interface. Lisa's particular interest in cybersecurity for medical devices stems from her oldest daughter's battle with chronic pain due to a pancreatic birth defect; after over 20 hospital stays and two major surgeries, she has finally experienced relief with an implanted neurostimulator.

Lisa earned her BS in computer science at the University of Wyoming, where she worked in the College of Engineering and helped build one of the first computer networks in the state. She and her husband of 31 years have four young adult children. Their oldest son is a Marine Sergeant, their younger son is an Army Lieutenant, their oldest daughter is a junior at Lesley University studying Fine Art, and their youngest daughter is a high school senior, dually enrolled as a college sophomore, planning to study pre-med.

Pamela Winer Goldberg, MBA

President and CEO
Medical Device Innovation Consortium (MDIC)
pgoldberg@mdic.org

Pamela Goldberg is an internationally recognized leader in healthcare technology innovation and entrepreneurship. As president and CEO of the Medical Device Innovation Consortium (MDIC), she provides strategic insight and guidance to help solve complex regulatory, scientific, and reimbursement challenges in the medical device industry. She brings her expertise in advancing technology-based solutions to develop unique strategies to help ensure innovative technology is readily available to patients across the country.

Prior to joining MDIC in 2018, Pamela served as CEO of the Massachusetts Technology Collaborative and the first woman to lead the organization in its 30-year history. Pamela worked closely with industry, academic and government leaders to advance technology-based solutions that improved the health care system, expanded high-speed Internet access and strengthened the growth and development of the state's technology sector with specific focus on digital health, data analytics, robotics, and cybersecurity.

Pamela also previously as the Director of The Center for Entrepreneurial Leadership at Tufts University, a program she launched to drive innovation for the university. Through her leadership, the program grew to over 500 students per year, and supported the start of over 50 businesses in Massachusetts. Recognized for her innovative efforts, Pamela was awarded the Acton Foundation's National Teaching Award for Entrepreneurship and established the school's nationally recognized business plan competition.

Pamela is advisor and board member to several technology startups and earlier in her career launched three start-up ventures: a music production company, a women's history organization and a hospice. At the start of her career, she was an investment banker at Citibank and then launched the investment banking division of State Street Bank.

Pamela received her BA from Tufts University and MBA from Stanford University.

Julian M. Goldman, MD

Medical Director of Partners Biomedical Engineering, Anesthesiologist, and Director, Program on Medical Device Interoperability & Cybersecurity
Massachusetts General Hospital / Partners HealthCare System
jmgoldman@mgh.harvard.edu

Dr. Julian Goldman, MD is an anesthesiologist at the Massachusetts General Hospital, the Medical Director of Biomedical Engineering for the Partners HealthCare System, and Director of the Program on Medical Device Interoperability and Cybersecurity (MD PnP).

Dr. Goldman performed clinical anesthesia and medical device informatics training at the University of Colorado School of Medicine, and is Board Certified in Anesthesiology and Clinical Informatics. He served as a principal anesthesiologist in the MGH "OR of the Future," a multi-specialty operating room that studied diverse technologies and clinical practices prior to broader adoption. In 2004 he founded the MD PnP program at MGH to improve patient safety and accelerate innovation. The newly expanded MD PnP Lab provides a pre-clinical virtual hospital "sandbox" for collaboration on cybersecurity preparedness and response.

Dr. Goldman was a Visiting Scholar in the FDA Medical Device Fellowship Program and a chief medical officer of a medical device company. He serves in leadership roles in medical device standardization committees, including AAMI, ISO, and IEC, and is an Associate Editor of ACM Transactions on Computing for Healthcare.

Dr. Goldman's awards include the AAMI Foundation/Institute for Technology in Health Care Clinical Application Award, the International Council on Systems Engineering Pioneer Award, and the American College of Clinical Engineering award for Professional Achievement in Technology, and appointment as an IEEE EMBS Distinguished Lecturer.

E-card: www.jgoldman.info

John Gomez

Chief Executive Officer
Sensato
John.gomez@sensato.co

John Gomez started his career in cybersecurity in high-school, having breached the security of a time-share computer system. Since that time, John's career has taken many twists and turns, as a Police Officer, Special Operations Instructor, Microsoft employee, CTO of WebMD, CTO/President of AllScripts. Yet throughout the years, he has never lost his passion for cybersecurity.

Today, John is a highly sought-after speaker, strategist and attacker. He specializes in the safeguarding of critical systems and continues to work on advanced cybersecurity solutions and research. His current work is focused on safeguarding medical devices, developing solutions that evolve the United States ability to effectively fight a cyberwar and the application of artificial intelligence to automated countermeasures and real-time forensics. John is also the founder and CEO of Sensato, a two-time Top-500 Most Innovative Cybersecurity firm that focuses primarily in healthcare information technology cybersecurity and critical infrastructure.

Matthew Hazelett

Biomedical Engineer
Office of Device Evaluation
Implantable Electrophysiology Devices Branch
Matthew.Hazelett@fda.hhs.gov

Matthew Hazelett came to the Food and Drug Administration as a biomedical engineer within the Implantable Electrophysiology Devices Branch (IEDB) at the Center for Devices and Radiological Health (CDRH). His review areas include pacemakers, defibrillators, leads, supporting devices (programmers, home monitors, etc.), and cybersecurity.

Matthew earned a B.S. in biomedical engineering from the University of Rochester where he focused in electrical signals and systems. After graduation, he worked for a medical device research and development company in New Hampshire as a Test Engineer and then Test Manager overseeing device verification and validation testing.

Zack Hornberger, CISSP

Director of Cybersecurity & Informatics
Medical Imaging & Technology Alliance, a division of NEMA
zhornberger@medicalimaging.org

Zack Hornberger is the Medical Imaging & Technology Alliance (MITA) subject matter expert on cybersecurity and informatics. MITA is the leading trade association representing the manufacturers of medical imaging equipment and radiopharmaceuticals. His work is focused on the development of technical standards, cybersecurity policies, and improved cybersecurity in the healthcare sector. He worked previously with cybersecurity software company Security First Corp. where he designed and deployed secure architectures for Fortune 500 companies.

Zack earned a B.A. in English Language and Literature from the University of Maryland College Park. He also holds several industry certifications, including the Certified Information Systems Security Professional certification.

Ken Hoyme, MSEE

Director
Product Security
Boston Scientific
ken.hoyme@bsci.com

Ken Hoyme has over 35 years' experience in the design and development of safety-critical, real-time, fault-tolerant and secure systems in a variety of regulated domains, including medical systems, commercial and military avionics, industrial automation and space systems. He is a recognized expert in the field of systems engineering.

Recently returning to Boston Scientific, he works with internal and external stakeholders to drive and improve processes and practices for pre- and post-market cybersecurity risk management across the company's products and services. In that role he also regularly interacts with academic institutions and industrial consortia.

Hoyme is past co-chair of AAMI's Device Security Working Group which has developed guidance for the application of medical safety risk standard ISO 14971 to security risk management and he serves on AAMI's BI&T Editorial Board.

Prior to his return to Boston Scientific, Mr. Hoyme was a Distinguished Scientist at Adventium Labs, where his research focus was on safety and security-critical architectures and risk management methods for cyberphysical systems in a variety of domains, including medical devices and aerospace systems.

Prior to joining Adventium Labs, Mr. Hoyme was a Senior Fellow at Boston Scientific where he was the systems lead for the development of the LATITUDE Remote Patient Management system. He was also the technical focal for developing standards for interconnecting implantable cardiac device data to electronic medical records systems.

Prior to joining Boston Scientific, Ken spent 18 years at Honeywell's Corporate Research lab, where he was a Senior Fellow in their real-time computer systems group. He was awarded the H.W. Sweatt Award, Honeywell's highest technical recognition for his work on the Boeing 777.

Ken has been granted 48 US and 9 International patents. He is a member of IEEE and INCOSE. He received the Bachelors and Master's Degrees in Electrical Engineering from the University of Minnesota.

Jim Jacobson

Chief Product and Solution Security Officer
Siemens Healthineers

Jim Jacobson is the Chief Product and Solution Security Officer for Siemens Healthineers. Since 2012, he has been responsible for the global security program for the medical devices and associated IT systems, solutions and services that Siemens Healthineers develops, sells, maintains and supports.

Jim also sits on the Siemens Product and Solution Security Board responsible for governance and guidance for the security of the company's products, solutions and services in all sectors including industrial, power, energy, renewables and mobility, in addition to healthcare. He leads the board's work team responsible for the curriculum and training program in this area for Siemens employees worldwide. Prior to these roles, Jim has led medical device-related software development teams in ultrasound, laboratory diagnostics and informatics since 1990 at Siemens and other companies. Jim has a degree in physics from Oberlin College.

Michelle Jump, MS

Vice President of Cyber Program Initiatives
Nova Leah, Ltd
michelle.jump@novaleah.com

Michelle Jump is the Vice President of Cyber Program Initiatives at Nova Leah, Boston, MA (headquartered in Ireland) , where she is responsible for providing strategic leadership, training, and education to the medical device industry, and thought leadership in the area of medical device cybersecurity risk management in line with Nova Leah's core platform, SelectEvidence®. She helps medical device manufacturers meet the challenges of cybersecurity risk management and vulnerability monitoring using SelectEvidence® by better aligning with existing security standards, automating vulnerability monitoring, and more efficiently and accurately managing security risks.

Ms. Jump has a passion for bringing technology-based solutions to healthcare, actively participating in a variety of international and domestic standards development work, as well as serving as a panel member, session leader, and presenter at a variety of events to further solutions to the challenges of technology in healthcare. Ms. Jump also holds leadership positions in several working groups, including NTIA Software Transparency Task Group lead, AAMI Software working group co-chair, and AAMI Health Software Quality working group co-chair. She has also been a member of UL Standards Technology Panel, various AAMI technology-based working groups, the AAMI Standards Board and has participated as the primary U.S. industry representative for the International Medical Device Regulators Forum (IMDRF) on the Software as a Medical Device working group. Current leadership roles in the area of standards development include Project Lead for ISO 81001 Health Software and IT Systems Safety: Foundational Principles, Concepts, and Terms, and the Project Lead for AAMI TIR 75: Factors to Consider when Multi-Vendor Devices Interact via an Electronic Interface. Ms. Jump holds a Master of Science in Regulatory Science from the University of Southern California and a Master of Science in Biotechnology from California State University. She is also RAC certified and a Certified HIPAA Administrator.

Tara Larson- Technical Fellow, CISSP, HCISSP, CSSLP, CISM, CEH

Senior Principal Systems Engineer-
Medtronic
Tara.j.larson@medtronic.com

Tara Larson has been in various roles in Information and Product security for ~ 22 years. Tara is currently a Sr. Principal System Engineer and Technical Fellow at Medtronic. In the past 11 years at Medtronic, Tara has held various security roles ranging from application security to embedded system security. Tara is currently the lead technical security architect for the CRHF business unit. Tara has a B.S in Computer Science from the University of New Mexico. She has previously held various security roles at Los Alamos National Laboratory, Dept of Energy, and United Healthcare.

Tara is passionate about delivering secure medical device solutions that advance patient care and support active, flexible, and healthy lifestyles. In her current role she has championed and led a movement to embed robust security design into new development, perform intrusive, repetitive product security testing and enable secure innovation in patient follow up systems. Tara is a thought leader in areas such as modular software design, CBOM delivery, SDLC and advanced security architectures.

The uniqueness of Tara's contributions to secure development and secure data systems is evidenced by the work she does every day to secure implantable device ecosystems, that leverage many different technologies. Tara is known for developing a balanced security vision and designing secure systems for patients and customers.

In her spare time, she volunteers for "Girls who Code" and is a hockey mom to a budding NHL star…(hopefully)

Art Manion

Vulnerability Analysis Technical Manager
CERT Coordination Center
Software Engineering Institute
amanion@cert.org

Art Manion is the Vulnerability Analysis Technical Manager at the CERT Coordination Center (CERT/CC), part of the Software Engineering Institute at Carnegie Mellon University. He has studied software security and coordinated responsible vulnerability disclosure efforts since joining CERT in 2001. After gaining mild notoriety for saying "Don't use Internet Explorer" in a conference presentation, Manion now focuses on policy, advocacy, and rational tinkering approaches to software security, including standards development in ISO, OASIS, and FIRST. Prior to joining CERT Manion was the Director of Network Infrastructure at Juniata College.

Kevin McDonald

Director of Clinical Information Security
Mayo Clinic

Kevin McDonald, BSN, MEPD, CISSP, is the Director of Clinical Information Security at Mayo Clinic. His current responsibilities include the security of medical devices, identity and access management, security testing and cybersecurity assurance services across all of the Mayo Clinic sites. Kevin and his teams provide testing, mitigation and consultative services for devices and systems within Mayo Clinic and partner with external vendors to assist them in improving the security of their products. Their work has become nationally recognized with presentations at FDA Workshops, the Radiologic Society of North America Conference, Gartner Security and Risk Management Summit, AdvaMed, MedTech, NH-ISAC Summits, Archimedes Workshops, ICS2 and many others. Kevin also participates in, and brings Mayo Clinic's experiences to, several vendor security customer advisory boards as well as he is the Co-Chair of the Healthcare & Public Health Sector Coordinating Council Cybersecurity Task Group Joint Security Plan and a member of the HIMSS Cybersecurity, Privacy, and Security Committee. Kevin has 40 years of healthcare experience in both patient care and technology roles. His experience includes critical care and emergency nursing, education, nursing management, electronic medical record implementation, information technology and information security. He holds an undergraduate degree in Nursing and graduate degrees in Education and Information Systems.

Michael McNeil

Global Product Security & Services Officer
Royal Philips
Michael.mcneil@philips.com

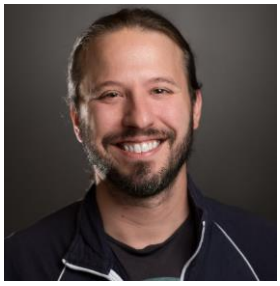
Michael C. McNeil is the Global Product Security & Services Officer for Royal Philips. McNeil leads global product security, ensuring consistent processes are deployed in the Healthcare market. McNeil was the former Global Chief Privacy & Security Officer at Medtronic; Chief IT Security Officer at Liberty Mutual Group; Global Chief Privacy Officer at Pitney Bowes, and Vice President, Chief Privacy Officer of Data Services for Reynolds & Reynolds.

McNeil, a security and privacy expert, recently provided expert testimony before Congress on Cybersecurity; and conducts training presentations worldwide.

McNeil is a member of the Department of Health & Human Services Healthcare Industry Cybersecurity Task Force; Chair of the MITA Cybersecurity Committee; Board member of National Health Information Sharing and Analysis Center, member of AAMI and MDISS.

Ben Miller

Vice President of Threat Operations
Dragon, Inc
bmiller@dragos.com



Ben Miller is VP of Threat Operations at the industrial cyber security company Dragos, Inc. where he leads a team of analysts in performing active defense inside of ICS/SCADA networks. In this capacity he is responsible for performing a threat hunting, incident response, and malware analysis mission for the industrial community.

Previous to his role at Dragos, Inc. Ben was the Associate Director, Electricity Information Sharing & Analysis Center (Electricity ISAC) and led cyber analysis for the sector. Ben was recognized as instrumental in building new capabilities surrounding information sharing and analytics in his five years at the E-ISAC. Prior to joining the E-ISAC, Ben built and led a team of 9 focused on Network Security Monitoring, forensics, and incident response at a Constellation Energy. His team received numerous accolades from industry and law enforcement. Ben has over 18 years' experience and currently holds the CISSP and GIAC GREM certifications. Ben has served in various roles including both planner and player roles in GridEx I, II, and III. He served as a facilitator of several NERC Task Forces including the Cyber Attack Task Force, and is an acknowledged contributor to NIST SP 800-150. Ben is an accomplished speaker in various venues including SANS, ICSJWG, ShmooCon and others. He was recognized by SANS as a 2017 Difference Maker Award Winner for his contributions to the electricity sector.

Colin Morgan, CISSP, CISM, GPEN

Director of Product Security & Services
Global Product Security & Services Program
Johnson & Johnson
CMorga48@its.jnj.com

Colin Morgan, Director of Product Security & Services at Johnson & Johnson, is responsible for leading the company's Global Product Security & Services Program. The Team's mission is to ensure all products of the Johnson & Johnson Family of Companies are built on Cybersecurity best practices and that Cybersecurity risks in marketed products are properly managed to support customer's safety and security.

Colin has worked in the Cybersecurity field for numerous organizations including the Central Intelligence Agency, and as a contractor for the National Oceanic & Atmospheric Administration. He is a featured speaker on Cybersecurity and is passionate about the integration of the competency across all industries. Colin has his B.S. in Computer Engineering from The College of New Jersey, a M.S. in Telecommunications from George Mason University, and is CISSP, CISM and GPEN certified.

Mike Nelson

VP of IoT Security
DigiCert, Inc.
Mike.Nelson@digicert.com

Mike Nelson is the VP of IoT Security at DigiCert, a leader in digital security. In this role, Mike oversees the company's strategic IoT market development for critical infrastructure industries. Mike frequently consults with organizations, contributes to media reports, and speaks at industry conferences about how technology can be used to improve cybersecurity for connected systems.

Before DigiCert, Mike spent his career in healthcare IT including time at the US Department of Health and Human Services, GE Healthcare, and Leavitt Partners. Mike's passion for the industry stems from his personal experience as a type 1 diabetic and his use of connected technology in his treatment.

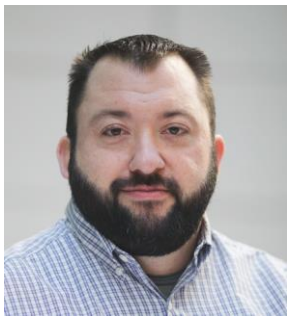
Scott T. Nichols, HCISPP, CHPSE, MCP

Director, Global Product Privacy and Security
Beckman Coulter/Danaher
stnichols@beckman.com

Mr. Nichols has over 20 years of experience in the Healthcare Information Technology industry. In his current role, he leads the Global Product Privacy and Security program at Beckman Coulter and across other Danaher Operating Companies. Focusing on privacy and security by design for Danaher's medical devices, diagnostics, life sciences, water quality, product identification and dental product portfolio's. Mr. Nichols is the chairman for the Danaher Global Product Privacy and Security Council and sits on multiple advisory boards inside out and outside of Danaher. Prior to Beckman Coulter/Danaher, Mr. Nichols was the Senior Director of Healthcare Information Services and HIPAA Security Officer for CHMB, an Allscripts partner and national electronic health records hosting provider. He has served as Director of IT and HIPAA Security Officer for multiple large health systems in California. Mr. Nichols holds certifications as a Healthcare Information Security and Privacy Practitioner and a Certified HIPAA Privacy Security Expert.

Jay Radcliffe, CISSP

Cyber Security Researcher
Thermo Fisher Scientific
Jay.radcliffe@thermofisher.com



Jay Radcliffe (CISSP) has been working in the computer security field for over 20 years. Coming from the managed security services industry as well as the security consultation field, Jay has helped organizations of every size and vertical secure their networks and data. Jay presented ground-breaking research on security vulnerabilities in multiple medical devices and was featured on national television as an expert on medical device cyber-security. As a Type I diabetic, Jay brings a lifetime of being a patient to helping medical facilities secure their critical data without compromising patient care. Not only is Jay a prolific public speaker, but also works with legal firms on expert witness consultation related to IoT and cyber security issues. Jay holds a Master's degree in Information Security Engineering from SANS Technology Institute, as well as a Bachelor's degree in Criminal Justice/Pre-Law from Wayne State University. SC Magazine named him one of the Top Influential IT Security Thinkers in 2013.

Linda Ricci

Associate Director ODE DH
ODE
FDA/CDRH
Linda.Ricci@fda.hhs.gov

Linda Ricci works in the Office of Device Evaluation on policy related to Digital Health and Software technologies. Ms. Ricci has also been the Chief for the Cardiac Diagnostic Devices Branch where she oversaw the premarket review for cardiac diagnostic, monitoring, and external defibrillation devices. Prior to joining the FDA, Ms. Ricci was a software developer in the medical device industry for cardiac monitoring devices. In addition, she has worked on artificial intelligence applications for the defense industry.

Ms. Ricci has degrees in Electrical Engineering and Medical Engineering.

.

Billy Rios, MBA, MS

Co-Founder
QED Secure Solutions
Billy.Rios@qedsecure.com

Billy was previously the founder of Whitescope LLC, which was acquired by QED Secure Solutions. QED Secure Solutions is a cybersecurity company focused on embedded device security. Billy is recognized as one of the world's most respected experts on emerging threats related to Industrial Control Systems (ICS), Critical Infrastructure (CI), and, medical devices. He discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. Billy provided the research that led to the FDA's first cyber security safety advisory and research which helped spur the FDA's pre-market cyber security guidance.

Billy is a contributing author to Hacking: The Next Generation, The Virtual Battlefield, and Inside Cyber Warfare. He currently holds a Master of Science in Information Systems, an MBA, and a Masters of Military Operational Arts and Science.

Aftin Ross, MSE, PhD

Senior Project Manager/Senior Science Health Advisor
Emergency Preparedness/Operations and Medical Countermeasures (EMCM)
Center for Devices and Radiological Health
Food and Drug Administration
Aftin.Ross@fda.hhs.gov

Aftin Ross is a senior project manager and senior science health advisor in the Emergency Preparedness/Operations and Medical Countermeasures program at the FDA's Center for Devices and Radiological Health (CDRH). In this role, she leads cross-disciplinary projects related to preparedness including medical device cybersecurity, respiratory protective devices, personal protective equipment, and incident response. Regarding cybersecurity, she has been a lead in CDRH's medical device cybersecurity efforts spearheading the execution of three FDA public workshops, serving on various interagency cybersecurity work groups, supporting numerous cross-stakeholder efforts (e.g. the 2017 healthcare cybersecurity task force report), managing CDRH's MITRE cybersecurity contract, and engaging in policy development as a member of the CDRH cybersecurity workgroup. Aftin earned a B.S. in mechanical engineering from the University of Maryland Baltimore County where she was a Meyerhoff Scholar. She completed her graduate work at the University of Michigan earning a master's and PhD in biomedical engineering. After her graduate work, she completed a post-doctoral fellowship as a Whitaker International Fellow at the Karlsruhe Institute of Technology in Karlsruhe, Germany. In 2016, she completed the National Preparedness Leadership Initiative, an executive education program in the Harvard School of Public Health and Kennedy School of Government.

Dana-Megan Rossi, J.D.

Assoc. Director, Product Security Policy, Strategy & Incident Response
BD
dana-megan.rossi@bd.com

Dana-Megan Rossi leads the Product Security Policy & Strategy and Incident Response programs at BD. Her work focuses on strategic security operations and initiatives, collaborations and response preparedness to enhance the security of product to customers by design, in use and through partnership. She works to ensure the adoption of the BD Product Security Framework across business units and regions, and Product Security program initiatives across the BD product portfolio, including integration of risk management and strategic intelligence, security awareness and trainings, and post-market security operations. Ms. Rossi previously served as the Product Security Officer for the Technology Solutions and Digital Health business units at BD. Ms. Rossi brings extensive experience in managing global product cybersecurity incident response, having previously led incident response coordination and preparedness, including the GE Product Security Incident Response Team (PSIRT) and crisis-level cybersecurity response plans and processes, drafted and led tabletop exercises, and coordinated multi-stakeholder security responses. Prior to GE, Ms. Rossi created and led a cybersecurity law & policy forum for corporate counsel, bringing together legal counsel, senior U.S. government advisors and IT professionals for cyber preparedness. Ms. Rossi currently serves as the Health Care and Public Health Sector Chief for InfraGard's National Capital Region, and is a member of the Cyber Health Working Group. She holds a Juris Doctor from Loyola University New Orleans, is licensed to practice law in New York, and earned her undergraduate degree from American University. She has also completed cyber intelligence training with the NCFTA and the Domestic Security Alliance Council. Ms. Rossi regularly speaks on product security matters and participates in public-private collaborations and cyber war game engagements.

Zach Rothstein, J.D.

Vice President
Technology & Regulatory Affairs
AdvaMed
zrothstein@advamed.org

Zach Rothstein is Associate Vice President for Technology & Regulatory Affairs at the Advanced Medical Technology Association (AdvaMed). In this position, Zach advocates for medical device regulatory policies that are transparent, predictable, consistent, timely, and science-based, with an emphasis on U.S. Food and Drug Administration ("FDA") and legislative activities. Zach's particular areas of focus include digital health, medical device software, cybersecurity, labeling, and postmarket surveillance.

Prior to joining AdvaMed, Zach was Deputy Senior Counsel for Public Policy at Samsung Electronics where he was responsible for the company's medical device and healthcare regulatory and policy issues. In this position, Zach counseled Samsung's global business units through all stages of product development on U.S. regulations affecting digital health, Health IT, and medical devices. Zach also planned and executed the company's FDA and healthcare regulatory and legislative policy objectives. While at Samsung, Zach served on the Board of Directors for the Personal Connected Health Alliance (formerly Continua) and the Consumer Electronics Association's Health and Fitness Technology Division.

Zach earned his J.D. from The Catholic University of America, where he was a Notes and Comments Editor of the Law Review, President of the Moot Court Board, and won first place and best brief awards at the 2009 National Telecommunications Moot Court Competition. Zach received his B.A. in political science and criminal justice from Indiana University, Bloomington.

Zach is an active member of the Food and Drug Law Institute, teaches an introduction to FDA law class at the Johns Hopkins University, and was recognized by i3 magazine as a digital health and fitness innovator.

Suzanne B. Schwartz, MD, MBA

Associate Director for Science & Strategic Partnerships
Office of the Center Director
Center for Devices & Radiological Health (CDRH), US FDA
Suzanne.Schwartz@fda.hhs.gov

Previously a surgical faculty member in clinical academia and medical director of a medtech startup, Suzanne joined FDA in October 2010 as a Commissioner's Fellow serving as a medical officer in CDRH's Division of Surgical Devices – Plastics and Reconstructive Surgery Branch. In 2012, she took on the role of Director of CDRH's Emergency Preparedness and Medical Countermeasures (EMCM) Program and has subsequently become the Center's Associate Director for Science & Strategic Partnerships. Suzanne's portfolio includes programmatic efforts in medical device cybersecurity, extending beyond incident response to include increasing awareness, educating, outreach, partnering and coalition-building within the Healthcare and Public Health Sector (HPH) as well as fostering collaborations across other parts of government and the private sector. Suzanne has been recognized with an award for Excellence in Innovation at FDA's Women's History Month on March 1st 2018 for her work in Medical Device Cybersecurity.

Suzanne chairs the CDRH Cybersecurity Working Group which is tasked with formulating policy on medical device cybersecurity on behalf of the Agency. She also serves as co-chair of the Government Coordinating Council (GCC) for the HPH Critical Infrastructure Sector, focusing on the sector's healthcare cybersecurity initiatives.

Suzanne earned an MD from Albert Einstein College of Medicine of Yeshiva University in New York in 1988, trained in General Surgery and Burn Trauma at the New York Presbyterian Hospital - Weill Cornell Medical Center; an executive MBA from NYU Stern School of Business in 2012, completed Cohort X of the National Preparedness Leadership Initiative – Harvard School of Public Health & Harvard Kennedy School of Government executive education in June 2013, and earned in September 2018 a certificate of mastery for completion of requirements at the Federal Executive Institute – Leadership for a Democratic Society.

Alain Silk, PhD

Acting Diabetes Diagnostic Devices Branch Chief
CDRH

Alain.Silk@fda.hhs.gov

As a medical device regulatory professional, Alain Silk works on behalf of the American people to protect and promote the public health. He is currently a Reviewer at the US Food and Drug Administration (FDA), where he uses his broad research background to ensure timely patient access to high-quality medical devices. “In my job I see first-hand the added value that regulation plays in assuring the safety and effectiveness of these devices,” he says.

Since joining FDA in early 2014 he has focused on in-vitro diagnostic (testing) devices as a member of the Division of Chemistry and Toxicology Devices in the Center for Devices and Radiological Health.

He is a trained cell biologist with college teaching experience. Alain received his Ph.D. from the University of California at San Diego, conducted post-doctoral training in the Knight Cancer Institute at Oregon Health and Science University, and has held teaching appointments in the Biology departments of both Lewis & Clark College (Portland, OR) and American University (Washington, D.C.). Alain was diagnosed with Type 1 diabetes in 2006.

Greg Singleton, MS

Director
Health Sector Cybersecurity Coordination Center (HC3)

Greg.singleton@hhs.gov

Greg Singleton is the Director of the Health Sector Cybersecurity Coordination Center (or HC3), an HHS group working to improve Cybersecurity in the Health sector through information sharing and coordination. Prior to joining HHS as the Director for the HC3, Greg worked at the Department of Energy (DOE), most recently serving as a Senior Advisor, working on power grid cybersecurity, critical infrastructure protection, power grid resilience, and managing clean energy entrepreneurship programs. Originally from Ohio, Greg graduated from the University of Virginia with a Bachelor's in Systems Engineering, and received Masters' degrees from MIT in Political Science and Technology and Policy.

Rob Suárez*, HCISPP*

Director, Product Security
BD (Becton, Dickinson & Company)
rob.suarez@bd.com

Roberto (Rob) Suarez is a cybersecurity and privacy professional in the medical device and healthcare IT industry. At BD, Rob established and leads a center of excellence for Product Security that drives process, capability and maturity to build products that are secure by design, in use and through partnership with transparency and control in mind. Giving product team's exposure to cybersecurity training and events, promoting the use of tools and solutions that provide customers a consistent security experience, building in-house expertise and promoting a company-wide community of practice for product security are what Rob is passionate about pursuing. Rob started his career in the Software Engineering department of Siemens Corporate Research and then worked on remote service platforms for medical devices in Siemens Healthcare Diagnostics. Through his technical knowledge acquired during these experiences and his personal initiative, Rob became a Product Security Expert and Program Manager for Siemens Healthcare where he educated product development teams on product security activities, institutionalized policies and procedures as well as supported secure product design and architecture. Rob was a member of the Department of Health and Human Services (HHS) Health Care Industry Cybersecurity Task Force which delivered its final report to U.S. Congress in June of 2017. The task force was created by the Cybersecurity Information Sharing Act of 2015 and is comprised of government and private industry leaders who are innovators in technology and pioneers in health care. The task force looked across industries and sectors to find the best ways organizations of all types are addressing the cybersecurity challenge in order to draw lessons that can be applied to the healthcare sector. As a continuation of the task force, established under U.S. Presidential Policy Directive 21, Rob served as a Chair for the Healthcare Sector Coordinating Council (HSCC) Med Tech Cybersecurity Risk Management Task Group aimed at establishing a voluntary framework, maturity model, and joint plan for improving cybersecurity for medical technology. In the spirit of transparency and collaboration, Rob has worked closely with the FDA on the common vulnerability scoring system for healthcare and sharing security best practices, in addition to the Department of Homeland Security on coordinated vulnerability disclosure. Rob is a Certified HealthCare Information Security and Privacy Professional (HCISPP) and has degrees in Computer Science from Montclair State University.

Nastassia Tamari

Sr. Manager, Product Security Incident Response and Vulnerability Management
Becton Dickinson
Nastassia.Tamari@bd.com

Nastassia Tamari currently leads the Product Security Incident Response Team (PSIRT) and is responsible

for establishing product security coordinated disclsoure processes, industry collaboration and partnership with key stakeholders, and cyber preparedness for all of BD's software enabled products. These initiatives ensure that BD continuously strives to advance a holistic approach to build products which are secure by design, in use and through partnership. Additionally, Nastassia leads product security crisis management response plans and processes, leads tabletop exercises, and coordinated multi-stakeholder communication to ensure wide-spread adoption and alighment across the business.

Nastassia Tamari earned a B.A. in Communication from San Diego State University. She completed her graduate work at Boston University earning an M.S. in Journalism.

Commented [AMR1]: Insert photograph here. Photo should not be larger than 2" by 2"

Michelle Tarver, M.D., Ph.D.

Director, Patient Science and Engagement Program
Office of the Center Director
Center for Devices and Radiological Health
michelle.tarver@fda.hhs.gov

Michelle Tarver is the Director of the Patient Science and Engagement Program at the Center for Devices and Radiological Health (CDRH). The Patient Science and Engagement Program fosters innovative approaches to collecting, analyzing and integrating the patient perspective in the development, evaluation and surveillance of medical devices, including digital health technologies. Through her leadership, CDRH is encouraging the integration of the patients' perspectives throughout the total product lifecycle of medical devices to further inform the regulatory and healthcare decision-making process. Dr. Tarver collaboratively works on developing the science of patient input (which includes patient-reported outcomes and patient preference information) to inform medical device development, evaluation, and surveillance. She also leads the CDRH Patient Engagement Advisory Committee efforts, an advisory panel comprised entirely of patients and caregivers providing their perspectives on general issues related to the regulation of medical devices. In addition to her experience in patient-focused efforts, Dr. Tarver has extensive experience in premarket and postmarket review of various medical devices, developing guidance documents and standards, fostering external collaborations, and designing workshops and other public meetings.

Dr. Tarver attended Spelman College in Atlanta, GA where she received a B.S. in biochemistry. She completed the M.D./Ph.D. program at The Johns Hopkins University Bloomberg School of Public Health (Ph.D. in clinical epidemiology) and The Johns Hopkins University School of Medicine. Following her internal medicine internship, she completed a residency in ophthalmology with fellowship training in ocular inflammation (uveitis) both at the Wilmer Eye Institute (Johns Hopkins). As an epidemiologist and board-certified ophthalmologist, she has worked on longitudinal epidemiological studies, developing patient-reported outcome measures as well as surveys to capture patient preferences with medical devices. Her research has resulted in numerous peer-reviewed publications and published book chapters. As a dedicated clinician, she continues to evaluate and treat ophthalmology patients at Solomon Eye Associates.

Jason Tugman, CISSP, CRISC, CCSK, ITPM

Vice President, Cyber Risk Engineering
Axio Global
Jtugman@axio.com

Jason Tugman is a Vice President of Axio. Axio is a cyber resilience optimization firm that helps organizations implement more comprehensive cyber risk management based on an approach that harmonizes cybersecurity technology/controls and cyber risk transfer. Jason's responsibilities center on delivering all facets of Axio's cyber risk engineering approach to clients, with a specific focus on cyber risk quantification, and cyber program design and implementation. Jason's work leverages NIST Cybersecurity Framework (CSF), DOE Cybersecurity Capability and Maturity Model (C2M2), and CERT Resilience Management Model (CERT-RMM).

Previously, Jason was a Senior Cyber Risk and Strategy consultant working with large financial and energy companies where he developed cyber resiliency strategy, cyber risk quantification programs, and analyzed Return on Security Investment (ROSI). Additionally, Jason served as a Program Manager where he led a team to develop, maintain, and perform a CSF-based pre-binding cybersecurity assessment for a Lloyds of London-backed $200mm cyber insurance policy for Critical Infrastructure. Prior to this, Jason was a Group Leader at the MITRE Corporation, where he spent 9 years leading teams in the development of program and technology prototypes for the Department of Defense and Intelligence Community.

Jason has a passion for cyber risk quantification and seeks to improve the science of risk-based decision making. He conducts ongoing research on developing a methodology where cyber risks and cybersecurity assessments can be aligned and then mapped to a cyber threat vector ontology, thus enabling business-risk-to-threat-vector control strength quantification. He maintains his Certified Information System Security Professional (CISSP) and Certified in Risk and Information Systems Control (CRISC) certifications and holds certificates for Certificate of Cloud Security Knowledge (CCSK) and Insider Threat Program Manager (ITPM). Jason is a veteran of the United States Marine Corps.

Eugene Vasserman, PhD

Associate Professor of Computer Science
Kansas State University
eyv@k-state.edu

Eugene Vasserman is a subject matter expert in cybersecurity and computer networking. He came to OSEL at the Food and Drug Administration in 2016 as an ORISE fellow. In 2018, he returned as a Senior Staff Fellow to CDRH. He serves as a cybersecurity specialist consultant for device and software reviews and is a member of the CyberSecurity Working Group (CSWG), helping with cybersecurity incident response. He served on the St. Jude Medical Cybersecurity Response Team, which received the Commissioner's Special Citation for their work.

In his spare time, Eugene is an Associate Professor in the Department of Computer Science at Kansas State University and is the director of the university-wide Center for Information and Systems Assurance. His research has resulted in over 40 peer reviewed publications in computer science, psychology, and education. His public service history includes over 30 conference program committees and national and international standards committees.

Eugene received a B.S. in Biochemistry and Neuroscience (with a Computer Science minor) from the University of Minnesota in 2003. His M.S. and Ph.D. in Computer Science are also from the University of Minnesota, in 2008 and 2010, respectively. His current research is chiefly in various aspects of security for medical and other cyber-physical systems, security usability, and user education. His past work spans the gamut from security vulnerabilities emergent from the BGP infrastructure of the internet, to energy depletion attacks in low-power systems, to secure hyper-local social networking, to privacy and censorship resistance on a global scale, supporting billions of concurrent users.

Chad Waters

Senior Cybersecurity Engineer
Health Devices Group
ECRI Institute
cwaters@ecri.org

Chad Waters is a senior cybersecurity engineer in the Health Devices group at ECRI Institute. In this role, he evaluates medical devices, develops practical guidance, and consults with healthcare facilities about medical technologies. With 13 years of experience in IT security and network engineering, he is a subject matter expert in medical device cybersecurity and healthcare IT. He holds a Bachelor's of Science degree in Information Technology from Rochester Institute of Technology.

Beau Woods

Cyber Safety Advocate
I Am The Cavalry (dot org)
beauwoods@gmail.com

Beau Woods is a leader with the I Am The Cavalry grassroots initiative, a Cyber Safety Innovation Fellow with the Atlantic Council, Entrepreneur in Residence at the US Food and Drug Administration, and Founder/CEO of Stratigos Security. Beau has consulted with Global 100 corporations, the White House, members of Congress, foreign governments, and NGOs on some of the most critical cybersecurity issues of our time. Beau's focus is on Internet of Things (IoT) technologies where cybersecurity intersects public safety and human life issues, including healthcare, automotive, energy, oil and gas, aviation, transportation, and other sectors. Beau is a published author, frequent public speaker, often quoted in media, and is often engaged for public or private speaking venues.

Ashley S. Woyak, CISM

Business Information Security Officer
IT Security & Risk Management
Baxter International Inc.
Ashley_Woyak@baxter.com

Ashley Woyak serves as Business Information Security Officer (BISO) for Baxter International Inc. She is passionate about healthcare cybersecurity and shares her expertise with industry organizations that establish cybersecurity guidance and standards for medical devices. Ashley is a frequent speaker at major conferences on a wide range of healthcare cybersecurity topics, such as the Dark Web of medical records. Prior to joining Baxter, Woyak worked in the Cybersecurity Advisory Practice at Ernst & Young. She served in the United States Army as an Intelligence Manager and was deployed to Afghanistan twice. She is on the Executive Committee for the Healthcare and Public Health Sector Coordinating Council's (HSCC) Cybersecurity Working Group (CWG) and serves as Advisory Board Member for Bits N' Bytes, a non-profit organization that teaches school-aged children and senior citizens about the importance of cybersecurity. She is a Certified Information Security Manager (CISM) and has a bachelor's degree in law from Marquette University. Woyak is currently an MBA candidate at the University of North Carolina – Chapel Hill.

Ken Zalevsky

Head of Medical Device CyberSecurity
Bayer

Ken Zalevsky is the Head of Bayer Radiology Medical Device CyberSecurity, and his role includes leading the Medical Device CyberSecurity Function along with managing advanced research partnerships and collaboration projects with leading hospitals and key global opinion leaders. Ken is the Chair of the CyberSecurity working Group of DITTA (Global Diagnostic Imaging Healthcare IT & Radiation Therapy Trade

Association), and an active member of the CyberSecurity teams of MITA (Medical Imaging and Technology Alliance), and AdvaMed (Advanced Medical and Technology Association).

Ken is a certified CyberSecurity Leader (Carnegie Mellon University) and has over thirty years of professional and leadership experience, with the last sixteen years in the medical device industry. Ken holds undergraduate and graduate degrees from Carnegie Mellon University and attended the executive management program at Harvard Business School.

Ken has been a featured speaker on protected health information compliance strategy and medical device cybersecurity at national events including the Medical Device R&D

Summit, MEDSec 2016 in Silicon Valley, and in various industries, including the Association for Iron and Steel Technology (AIST). Ken has also authored various whitepapers and articles, including an article appearing in the January/February edition of HealthCare Business News on medical device cybersecurity, and multiple white papers in cooperation with industry trade associations.

Margie Zuk, M.S.

Senior Principal Cybersecurity Engineer
The MITRE Corporation
mmz@mitre.org

Margie Zuk is a Senior Principal Cyber Security Engineer at the MITRE Corporation, with over 30 years of cyber security experience. She is currently the Cyber Engagement Lead for Healthcare in the Cyber Solutions Technical Center, where she leads MITRE's support to the FDA CDRH on Medical Device Cyber Security and Preparedness and Response.

As the Industry Collaboration Department Head for many years, Margie led the evolution of the cyber standards work at MITRE from the launch of CVE to the structured threat work with STIX and TAXII. She led cross sponsor initiatives and cyber partnerships with senior leaders across government and industry to establish governance models and to evolve the cyber security standards strategy. Prior to this, Margie led MITRE's support to the National Information Assurance Partnership (NIAP). She was an initial member of the Common Evaluation Methodology Editorial Board and participated in the development of the US scheme for the Common Criteria.

Margie has a Bachelor of Arts in Mathematics from the College of Mt. St. Vincent and a Master of Science in Computer Science from Stevens Institute of Technology.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Title: Child Care and Development Fund (CCDF) State Monitoring Compliance Demonstration Packet.

OMB No.: New.

Description: The proposed data collection form is designed as part of the how they, as block-grant recipients, will choose to demonstrate compliance.

Respondents: 51 States and Territories triennially.

Activity; Proposed Information Collection Comment Request

ANNUAL BURDEN ESTIMATES

Instrument	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
Compliance Demonstration Chart	17	1	16	272
Document Submission Chart	17	1	80	1,360

Estimated Total Annual Burden Hours: 1,632 hours.

In compliance with the requirements of the Paperwork Reduction Act of 1995 (Pub. L. 104–13, 44 U.S.C. chap 35), the Administration for Children and Families is soliciting public comment on the specific aspects of the information collection described above. Copies of the proposed collection of information can be obtained and comments may be forwarded by writing to the Administration for Children and Families, Office of Planning, Research and Evaluation, 330 C Street SW, Washington DC 20201. Attn: ACF Reports Clearance Officer. Email address: *infocollection@acf.hhs.gov.* All requests should be identified by the title of the information collection.

The Department specifically requests comments on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information; (c) the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology. Consideration will be given to comments and suggestions submitted within 60 days of this publication.

Robert Sargis,

Reports Clearance Officer.

[FR Doc. 2018–22700 Filed 10–17–18; 8:45 am]

BILLING CODE 4184–43–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA–2018–D–3443]

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff; Availability

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of availability.

SUMMARY: The Food and Drug Administration (FDA or Agency) is announcing the availability of the draft guidance entitled ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.'' As more medical devices are becoming interconnected, cybersecurity threats have become more numerous, more frequent, more severe, and more clinically impactful. There is a need to provide manufacturers with specific technical recommendations (*e.g.*, appropriate threat modeling and other premarket testing) to help ensure device cybersecurity. The updates to the existing ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices'' guidance is anticipated to better protect against risks, such as ransomware campaigns, that could disrupt clinical operations and delay patient care and risks, such as exploiting a vulnerability that enables attacks on multiple patients. This draft guidance is not final nor is it in effect at this time.

DATES: Submit either electronic or written comments on the draft guidance by March 18, 2019 to ensure that the Agency considers your comment on this draft guidance before it begins work on the final version of the guidance.

ADDRESSES: You may submit comments on any guidance at any time as follows:

Electronic Submissions

Submit electronic comments in the following way:

- Federal eRulemaking Portal: *https:// www.regulations.gov.* Follow the instructions for submitting comments. Comments submitted electronically, including attachments, to *https:// www.regulations.gov* will be posted to the docket unchanged. Because your comment will be made public, you are solely responsible for ensuring that your comment does not include any confidential information that you or a third party may not wish to be posted, such as medical information, your or anyone else's Social Security number, or confidential business information, such as a manufacturing process. Please note that if you include your name, contact information, or other information that identifies you in the body of your comments, that information will be posted on *https://www.regulations.gov*.

- If you want to submit a comment with confidential information that you do not wish to be made available to the public, submit the comment as a written/paper submission and in the manner detailed (see ''Written/Paper Submissions'' and ''Instructions'').

Written/Paper Submissions

Submit written/paper submissions as follows:

- *Mail/Hand delivery/Courier (for written/paper submissions):* Dockets Management Staff (HFA–305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.

- For written/paper comments submitted to the Dockets Management Staff, FDA will post your comment, as well as any attachments, except for information submitted, marked and identified, as confidential, if submitted as detailed in ''Instructions.''

Instructions: All submissions received must include the Docket No. FDA– 2018–D–3443 for ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.'' Received comments will be placed in the docket and, except for those submitted as ''Confidential Submissions,'' publicly viewable at *https://www.regulations.gov* or at the Dockets Management Staff between 9 a.m. and 4 p.m., Monday through Friday.

- Confidential Submissions—To submit a comment with confidential information that you do not wish to be made publicly available, submit your comments only as a written/paper submission. You should submit two copies total. One copy will include the information you claim to be confidential with a heading or cover note that states ''THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION.'' The Agency will review this copy, including the claimed confidential information, in its consideration of

comments. The second copy, which will have the claimed confidential information redacted/blacked out, will be available for public viewing and posted on *https://www.regulations.gov*. Submit both copies to the Dockets Management Staff. If you do not wish your name and contact information to be made publicly available, you can provide this information on the cover sheet and not in the body of your comments and you must identify this information as ''confidential.'' Any information marked as ''confidential'' will not be disclosed except in accordance with 21 CFR 10.20 and other applicable disclosure law. For more information about FDA's posting of comments to public dockets, see 80 FR 56469, September 18, 2015, or access the information at: *https://www.gpo.gov/fdsys/pkg/FR-2015-09-18/pdf/2015-23389.pdf*.

Docket: For access to the docket to read background documents or the electronic and written/paper comments received, go to *https://www.regulations.gov* and insert the docket number, found in brackets in the heading of this document, into the ''Search'' box and follow the prompts and/or go to the Dockets Management Staff, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.

You may submit comments on any guidance at any time (see 21 CFR 10.115(g)(5)).

An electronic copy of the guidance document is available for download from the internet. See the **SUPPLEMENTARY INFORMATION** section for information on electronic access to the guidance. Submit written requests for a single hard copy of the draft guidance document entitled ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices'' to the Office of the Center Director, Guidance and Policy Development, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, Rm. 5431, Silver Spring, MD 20993–0002 or the Office of Communication, Outreach, and Development, Center for Biologics Evaluation and Research, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 71, Rm. 3128, Silver Spring, MD 20993–0002. Send one self-addressed adhesive label to assist that office in processing your request.

FOR FURTHER INFORMATION 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, or Stephen Ripley, Center for Biologics Evaluation and Research, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 71, Rm. 7301, Silver Spring, MD 20993, 240–402–7911.

SUPPLEMENTARY INFORMATION:

I. Background

The need for effective cybersecurity to assure medical device functionality and safety has become more important with the increasing use of wireless, internet- and network-connected devices, and the frequent electronic exchange of medical device-related health information. In addition, cybersecurity threats to the healthcare sector have become more frequent, more severe, and more clinically impactful. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the United States and globally. Such cyberattacks and exploits can delay diagnoses and/or treatment and may lead to patient harm.

Although FDA issued guidance addressing recommendations for device cybersecurity information in premarket submissions in 2014,[1] the rapidly evolving landscape, and the increased

[1] ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices—Guidance for Industry and Food and Drug Administration Staff'' at *https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190*.

understanding of the threats and their potential mitigations necessitates an updated approach. This draft guidance is intended to provide recommendations to industry regarding cybersecurity device design, labeling, and the documentation that FDA recommends be included in premarket submissions for devices with cybersecurity risk. These recommendations can facilitate an efficient premarket review process and help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats.

FDA plans to hold a public workshop on January 29th and January 30th, 2019.[1] FDA seeks to bring together diverse stakeholders to discuss, in- depth, the draft guidance, ''Content of

Premarket Submissions for Management of Cybersecurity in Medical Devices'' and the subtopic of the draft guidance regarding a Cybersecurity Bill of Materials (CBOM), which can be a critical element in identifying assets, threats, and vulnerabilities. **II. Significance of Guidance**

This draft guidance is being issued consistent with FDA's good guidance practices regulation (21 CFR 10.115). The draft guidance, when finalized, will represent the current thinking of FDA on Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. 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. This guidance is not subject to Executive Order 12866.

III. Electronic Access

Persons interested in obtaining a copy of the draft guidance may do so by downloading an electronic copy from the internet. A search capability for all Center for Devices and Radiological Health guidance documents is available at *https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/default.htm.* This guidance document is also available at *https://www.regulations.gov* or

https://www.fda.gov/BiologicsBloodVaccines/ GuidanceComplianceRegulatoryInformation/default.htm. Persons unable to download an electronic copy of ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices'' may send an email request to *CDRH-Guidance@fda.hhs.gov* to receive an electronic copy of the document. Please use the document number 1825 to identify the guidance you are requesting.

IV. Paperwork Reduction Act of 1995

This draft guidance refers to previously approved collections of information. These collections of information are subject to review by the Office of Management and Budget
(OMB) under the Paperwork Reduction

Act of 1995 (44 U.S.C. 3501–3520). The

[1] *https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm.*

collections of information in the following FDA regulations and guidance have been approved by OMB as listed in the following table:

21 CFR part or guidance	Topic	OMB control No.
807, subpart E	Premarket notification	0910–0120
814, subparts A through E	Premarket approval	0910–0231
814, subpart H	Humanitarian Device Exemption	0910–0332
812	Investigational Device Exemption	0910–0078
''De Novo Classification Process (Evaluation of Automatic Class III Designation)''.	De Novo classification process	0910–0844
801	Medical Device Labeling Regulations	0910–0485
820	Current Good Manufacturing Practice (CGMP); Quality System (QS) Regulation	0910–0073

V. Other Issues for Consideration

The Agency invites comments on the ''Content of Premarket Submissions for

Management of Cybersecurity in Medical Devices'' draft guidance, in general, and on the following topics, in particular:

- Definition of CBOM:

Æ Whether a CBOM should include both software and hardware components • Type of information and level of detail that should be included in a

CBOM

- Effective mechanisms for sharing

CBOM information • Format the CBOM should take: Æ Available formats that could be leveraged

Æ Whether multiple formats would be able to co-exist • Appropriate frequency for updating the CBOM

- Features of a CBOM that would make it automatically consumable

Dated: October 12, 2018.

Leslie Kux,

Associate Commissioner for Policy.

[FR Doc. 2018–22697 Filed 10–17–18; 8:45 am]

BILLING CODE 4164–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket Nos. FDA–2017–E–6698 and FDA– 2017–E–6699]

Determination of Regulatory Review Period for Purposes of Patent Extension; OCREVUS

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The Food and Drug Administration (FDA or the Agency) has determined the regulatory review period for OCREVUS and is publishing this notice of that determination as required by law. FDA has made the determination because of the submission of applications to the Director of the U.S. Patent and Trademark Office (USPTO), Department of Commerce, for the extension of a patent which claims that human biological product.

DATES: Anyone with knowledge that any of the dates as published (see the **SUPPLEMENTARY INFORMATION** section) are incorrect may submit either electronic or written comments and ask for a redetermination by December 17, 2018. Furthermore, any interested person may petition FDA for a determination regarding whether the applicant for extension acted with due diligence during the regulatory review

period by April 16, 2019. See ''Petitions'' in the **SUPPLEMENTARY INFORMATION** section for more information.

ADDRESSES: You may submit comments as follows. Please note that late, untimely filed comments will not be considered. Electronic comments must be submitted on or before December 17, 2018. The *https://www.regulations.gov* electronic filing system will accept comments until 11:59 p.m. Eastern Time at the end of December 17, 2018. Comments received by mail/hand delivery/courier (for written/paper submissions) will be considered timely if they are postmarked or the delivery service acceptance receipt is on or before that date. *Electronic Submissions*

Submit electronic comments in the following way:

- *Federal eRulemaking Portal: https://www.regulations.gov.* Follow the

instructions for submitting comments. Comments submitted electronically, including attachments, to *https:// www.regulations.gov* will be posted to the docket unchanged. Because your comment will be made public, you are solely responsible for ensuring that your comment does not include any confidential information that you or a third party may not wish to be posted, such as medical information, your or anyone else's Social Security number, or confidential business information, such as a manufacturing process. Please note that if you include your name, contact information, or other information that identifies you in the body of your comments, that information will be posted on *https://www.regulations.gov.*

- If you want to submit a comment with confidential information that you do not wish to be made available to the public, submit the comment as a written/paper submission and in the manner detailed (see ''Written/Paper Submissions'' and ''Instructions'').

Written/Paper Submissions

Submit written/paper submissions as follows:

- *Mail/Hand delivery/Courier (for written/paper submissions):* Dockets Management Staff (HFA–305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.
- For written/paper comments submitted to the Dockets Management Staff, FDA will post your comment, as well as any attachments, except for information submitted, marked and identified, as confidential, if submitted as detailed in ''Instructions.''

Instructions: All submissions received must include the Docket Nos. FDA– 2017–E–6698 and FDA–2017–E–6699 for ''Determination of Regulatory Review Period for Purposes of Patent Extension; OCREVUS.'' Received comments, those filed in a timely

Notes Section:

www.fda.gov/medicalcountermeasures