AdvaMed Cybersecurity Summit

Tuesday, December 5, 2023

Hogan Lovells US LLP
555 13th Street, NW
Washington, D.C. 20004

Welcome Reception
Monday, December 4, 2023 | 5:00 pm – 6:00 pm
AdvaMed Office | 1301 Pennsylvania Ave, NW Suite 400 Washington, DC

Tuesday, Dec 5, 2023

8:15 am – 9:00 am **Continental Breakfast and Registration Open**

9:00 am – 9:05 am **Welcome Remarks**

Anita Nosratieh, VP Technology & Regulatory, AdvaMed

9:05 am – 9:50 am **Regulatory Update**

Aftin Ross, Deputy Division Director (Acting), Division of All Hazards Response, Science and Strategic Partnerships (DARSS), CDRH, FDA

FDA will provide an update on medical device cybersecurity regulation, including implications of the omnibus, discussion of the recently released FDA Final Guidance, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions and a preview of what's ahead for FDA's cybersecurity policy focus in FY24 and beyond.

9:50 am - 10:50 am **FDA Implementation of Cybersecurity Requirements**

Chris Reed, Vice President, Product Security, Medtronic

Edison Alvarez, Sr. Director, Regulatory Strategic Planning for Cybersecurity, BD

Matt Hazelett, Cybersecurity Policy Analyst, Clinical and Scientific Policy Staff; Digital Health Center of Excellence Program Director, OPEQ, CDRH, FDA

Michelle Jump, CEO, MedSec

Colin Morgan, Managing Director, Apraciti, LLC

In this insightful session on FDA implementation of Cyber requirements, we will discuss the FDA perspective on essential reviewer training, navigation of challenges and opportunities and establishment of best practices. Industry representatives will share firsthand accounts – the good, the bad, the ugly – with FDA submission reviews involving cybersecurity with respect to the RTA/Focal Point program.

10:50 am – 11:05 am **Networking Break**

11:05 am – 11:50 am **Risk Scoring Methodology for Security Risk**

Michelle Jump, CEO, MedSec

Medical device manufacturers are under significant pressure to manage security risk, but with limited guidance for optimizing this process. In this session, we will discuss the difficulties associated with security risk scoring, one of the most challenging areas of security risk management, as well as opportunities in risk scoring methodology.

11:50 am – 12:35 pm **Cybersecurity is Now a Non-Negotiable With Mature Expectations. Here's How to Play Catch-Up if You're Feeling Behind the Eight-Ball.**

Naomi Schwartz, Senior Director of Cybersecurity Quality and Safety, MedCrypt

We will review regulations, standards, and guidelines that are foundational to a cooperative relationship between device manufacturers and device consumers, from procurement to device decommissioning. Medical device cybersecurity is a multi-stakeholder responsibility, and a common understanding of roles can lead to a constructive and successful partnership. After participating in this session, the learner will be able to define and articulate their cybersecurity maintenance needs.

12:35 pm – 1:30 pm **Networking Lunch**

1:30 pm – 2:30 pm

Mock FDA Cybersecurity Submission Review

Colin Morgan, Managing Director, Apraciti, LLC

Matt Hazelett, Cybersecurity Policy Analyst, Clinical and Scientific Policy Staff; Digital Health Center of Excellence Program Director, OPEQ, CDRH, FDA

In this session, attendees will have the opportunity to watch a mock FDA Cybersecurity Submission Review, covering many of the key topics in the latest Guidance, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. We will cover topics such as cybersecurity architecture diagrams, threat models, details of a cybersecurity management plan and cybersecurity quality systems.

2:30 pm – 3:15 pm

What Happens When You Do Get Hacked? Best Practices for Handling Worst Case Scenarios.

Randy Horton, Chief Solutions Officer, Orthogonal

Jim Jacobson, Chief Product and Solution Security Officer, Siemens Healthineers

What happens when, despite all technical, compliance and preventative measures in place, a medical device manufacturer gets hacked? We will explore a real-world example and the lessons learned and best practices for responding to a potential worst-case cybersecurity scenario.

3:15 pm – 3:45 pm

Public Sector Cybersecurity Requirements Heat Up: Increased Attention on StateRAMP and ATO Compliance

Joe Bartos, Senior Manager, Deloitte

Kate Upton, Senior Consultant, Deloitte

Cybersecurity requirements from the US Government for contracts with medical device manufacturers have always existed, but their enforcement has historically been inconsistent. In this session, we will discuss emerging trends in compliance requirements commonly seen in contracts with the U.S. Government when purchasing connected medical devices and platforms, such as federal and state Authorizations to Operate (ATO's) and the Federal and State Risk and Authorization Management Programs (FedRAMP and

StateRAMP). Our conversation will include a practical, day-in-the-life view of how medical device manufacturers can navigate government contracting for their devices. The session will include an overview of upticks the industry is seeing in this area, discussion on what is driving the change, and what makes these requirements difficult to implement and maintain. Coming out of this session, attendees will better understand how to interpret cybersecurity compliance requirements listed in their government contracts and what it takes to obtain and maintain authorizations to successfully sell and field their medical products within the US government.

3:45 pm **Closing Remarks**