AdvaMed Cybersecurity Summit
Wednesday, November 13, 2024

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 – 9:55 am	**FDA Regulatory Update** • FY25 priorities • Implementation health check • Other timely topics **Speakers:**
9:55 am – 10:45 am	**Navigating the FDA Cybersecurity Review Process** Submitting a connected device to the FDA has become significantly harder between eSTAR requirements, more deficiencies, and reviewers evaluating how manufacturers are securing devices. This session will cover the timeline for the evolution of the review process over the past several years, what manufacturers have experienced during this timeline, and common areas where manufacturers are continuing to face challenges in the review process that can result in costly review delays or negative decisions. **Speakers:** Matt Hazelett, Chief Regulatory Officer, MedSec Kristen Killheffer, Cybersecurity Regulatory Policy, Siemens Healthineers USA
10:45 am – 11:35 am	**Now, Who's Being Unreasonable Here? Sorting Out Best Practices and Decision Criteria for a *Reasonably Justified Regular Schedule*** We've all read it a millions time since it came out: "Design, develop, and maintain processes and procedures to provide a reasonable assurance the device and related systems are cybersecure, and make available post-market updates and patches to the device and related systems to address – a) on a

	reasonably justified regular cycle, known unacceptable vulnerabilities; and b) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks." So what criteria should we use to figure out the periodicity of a reasonably justified regular cycle? And what should differentiate acceptable and unacceptable vulnerabilities? The high-level answer is that the criteria should reflect the needs of: • Regulators • Our own businesses • What we would want for medical devices used by our own families In this session, we'll discuss emerging approaches to answering these questions, as well as similar efforts in other industries. This session format will engage both panelists and audience members in an insight-rich discussion that captures the best thinking of everyone in attendance. **Moderator:** Randy Horton, Chief Solutions Officer, Orthogonal **Speaker:** Oleg Yusim, Chief Product Security Officer, Illumnia Mike Nelson, VP of Digital Trust, DigitCert
11:35 am – 12:25 pm	**Leveraging Threat Model & Security Architecture views for effective product lifecycle security risk controls** Threat Modeling is both an art and a science and when mapped with accurate systemic Security Architecture representative views, the resulting symbiotic relationship can yield effective design input requirements as well as security risk control measures across the entire product lifecycle including supply chain and connected eco system. The presentation will cover how a well thought of continuous Threat Model approach can be a catalyst for any organization to derive effective risk control measures across a Secure Product Development Framework. **Speaker:** Sivaram Rajagopalan, Senior Cybersecurity Architect | Associate Director, Baxter Product Security

	Confirmed
12:25 pm – 1:35 pm	**Networking Lunch**
1:35 pm – 2:25 pm	**Securing Med Devices and the Impact of Ransomware on IoMT** **growing threat of rasomware** • Impact of ransomware attacks on med devies/networks • How to address challenges of securing connected med devices to prevent ransomware attacks • Practical examples of how Med Device Mfrs can respond to ransomware attacks involving their products **Speaker:** Chris Reed, Sr. Director of Cybersecurity Policy | Global Regulatory Affairs, Medtronic
2:25 pm – 3:15 pm	**Product Security Incident Response Team (PSIRT) - case study** How to effectively implement PSIRT process to support cybersecurity postmarket surveillance and how to leverage other existing quality processes such as Health Hazard Assessment and Field Corrective Action (FCA). **Speaker:** Manan Hathi, Sr. Manager, Digital Health Regulatory Policy and Intelligence, Stryker
3:15 pm - 4:05 pm	**Understanding IEC 81001-5-1: The new global standard driving regulatory expectations** There has been a lack of well-utilized global cybersecurity standards for medical devices for years. This led to a lack of clear alignment amongst regulators regarding what a good cybersecurity lifecycle process looks like. This has changed with the recent global embrace of IEC 81001-5-1 by many regulators across the globe. The US recognized this standard and recommends it as an accepted framework for an SPDF. The European Union has placed it on the harmonized standards list and major notified bodies are considering it mandatory. Perhaps most impactfully, Japan now requires conformance to this standard for all products sold in the country, not just for submitted products. This session will provide a foundation understanding of the standard, including notable challenge points for

	conformance. We will also provide clarification in certain areas of the standard that prove challenging to many users. **Speaker:** Michelle Jump, CEO, MedSec
4:05 pm – 4:55 pm	**Post-Quantum Cryptography: A strategy for medical device engineering** Cryptanalytically relevant quantum computers (quantum computers that can break today's asymmetric cryptography within the time the secret it guards is of value) are not a matter of if, but when. A transition to quantum-safe algorithms is a paradigm shift in the way the industry maintains the security of its operations and the safety of its patients. This transition will lead to deep engineering changes that will impact every technology stack that is used by medical devices. Compounding the problem is the overall lack of faith in these newly minted cryptographic algorithms. Contrast this with the solidity of RSA/ECC which are mature, well-studied algorithms that have withstood the test of time and countless cryptanalysts, and one begins to understand the technological risks of premature adoption of novel quantum-safe algorithms. A hybrid approach, of using both conventional as well as post-quantum crypto, provides a solid mitigator of this technical risk. Of course, that too comes with its own challenges---of supporting multiple cryptographic algorithms in the protocol suite. However, the bigger risk remains of doing nothing, of waiting till cryptanalytically relevant quantum computers become a real possibility. **Speaker:** Arnab Ray, Director, Product Cybersecurity, Abbott
4:55 pm – 5:00 pm	**Closing Remarks** *Anita Nosratieh, VP Technology & Regulatory, AdvaMed*