SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog July 2021

Topics covered in this issue:

- Current master list of FDA cyber-software guidance documents and links
- Discussing the SBOM - Software Bill of Material

FDA Cyber-software Guidance documents

In addition to official guidelines and standards, the FDA has released other documents and spoken on several topics that indicate the direction that the FDA is taking moving forward in regards to medical device cybersecurity. Perhaps the most consequential is and update of the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, expected to be released by the end of 2021. In addition, the FDA is working to respond to several developing recent threats to critical infrastructure cybersecurity, which became a clear and present danger in the period encompassing late 2020-mid 2021, including but not limited to the Solarwinds incursion, the ransomware attacks of the JBS meatpacking plant of June 2021, the Colonial Pipeline ransomware attack of June 2021, and the digital breach of a water treatment plant in Florida in February of 2021. In addition to these attacks on several sectors of critical infrastructure, the healthcare sector was affected directly, with ransomware attacks affecting Irish, New Zealand, and American (San Diego) healthcare providers in the spring of 2021. In addition to these attacks, which were comprehensive but not without precedent, new and unique related threats to medical device and healthcare cybersecurity have recently emerged, and the Biden administration is working with critical infrastructure oversight bodies such as the FDA to address and mitigate these threats and vulnerabilities. This has culminated in an Executive Order that was issued by President Biden on May 12, 2021. The Executive Order (EO 14028) is called Improving the Nation's Cybersecurity, and is a call for greater oversight, cooperation, and standardization in critical infrastructure by stakeholders in regards to cybersecurity. As a result of this Executive Order, the National Institute of Standards and Technology (NIST) has requested that relevant federal critical industry regulatory bodies, including the FDA, submit position papers on "standards and guideline to enhance software supply chain cybersecurity".

The FDA, in collaboration with the Center for Devices and Radiological Health (CDRH), released their response on May 26th of 2021, entitled "Response to NIST Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security (https://www.fda.gov/media/149954/download).

John Ward – Cyberblog July 2021

While this paper is not binding and contains no actionable regulation, it is an important snapshot of where the FDA is in terms of cybersecurity, the remediations and standards they consider important, and how they as a regulatory body will be adapting to the federal government's focus on critical infrastructure cybersecurity. Understanding this document, in tandem with the upcoming updated Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, will be invaluable to the medical device manufacturer community in navigating the rapidly-changing medical device cybersecurity regulatory landscape.

Prior to the Biden administration's Executive Order on critical infrastructure cybersecurity, largely made in response to several of the acute incidents listed above, the FDA was preparing to update their Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, with an estimated publishing date of the end of the calendar year 2021. In early 2021, Dr. Kevin Fu was named as the acting director for medical device cybersecurity at the FDA CDRH, a new position which indicates the increasing importance of cybersecurity within the medical device cybersecurity community. In prepared remarks given on March 17th, 2021 at a Regulatory Affairs Professional Society (RAPS) event entitled Cybersecurity Unauthorized, Dr. Fu indicated that an increasing amount of 510(k) submissions found to be "not substantially equivalent (NSE)" and postmarket approvals (PMA) are being found to be not approvable based on cybersecurity concerns alone.

According to Dr. Fu, as well as Dr. Suzanne Schwartz (Director of the CDRH) and Matthew Hazlett (Cybersecurity Policy Analyst at the FDA), the upcoming Content of Premarket Submissions for Management of Cybersecurity in Medical Devices will focus on two major topics: "Frontloading" new medical devices with the capabilities to be updated in an ongoing fashion, ensuring that they are able to adapt in a fluid and adaptable way to cybersecurity threats and vulnerabilities that may not have been known or even existed at the time of development. Dr. Fu indicated that this technique is known as ensuring that cybersecurity protections are "baked in and not bolted on", indicating that the FDA will be looking for robust and adaptable cybersecurity protections in medical devices during front-end development and implemented during the design and manufacturing phase, not as-needed to respond to specific threats as they appear when the device is already on the market. Dr. Fu was adamant at this event that the updated Content of Premarket Submissions for Management of Cybersecurity in Medical Devices will pertain largely to the means by which a medical device developer can communicate that they have implemented these features clearly to the FDA during the 510(k) submission process.

John Ward – Cyberblog July 2021

Discussing the SBOM - Software Bill of Material

Another significant focus of the upcoming Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, according to the FDA employees at the Cybersecurity Unauthorized event is the implementation of SBOMs (Software Bills of Material). An SBOM is a listing of software used in medical devices (although SBOMs will probably be common across critical infrastructures, not just within healthcare), including version history and patch history. The purpose of an SBOM is to make it easy to reference all software components in the event of an acute vulnerability for the customers, regulators, and medical device manufacturers. In an interview with medtechdrive.com (https://www.medtechdive.com/news/FDA-cyber-chief-talks-medical-device-risks-agency-priorities/602625/) on June 30th of 2021, Dr. Fu stated "…it's important that medical device manufacturers provide Software Bill of Materials (SBOMs) to better understand exposure to risk of both known and future vulnerabilities in third-party software in legacy devices," and "FDA is actively engaged with the International Medical Device Regulators Forum on Software Bill of Materials (SBOMs) and is supportive of the NTIA effort on SBOM. The FDA response to NIST also includes passages on FDA's support of SBOM as a key part of protecting medical device cybersecurity.

The document referenced by Dr. Fu in the final statement in the above paragraph is Response to NIST Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security (https://www.fda.gov/media/149954/download), which as mentioned in the introductory paragraph of this paper is a response by the FDA by a call from the NIST for regulators of critical industry to provide suggestions on critical infrastructure cybersecurity standardizations in the federal sector. This paper, submitted on May 26th of 2021, provides the FDA and CDRH's suggestions.

The paper begins by stating that critical infrastructure is more digitally vulnerable now than ever before, largely due to an increased reliance on cloud technology, and references ransomware attacks on healthcare systems in the past year. The report also mentions an instance where "ransomware remediation disrupted the clous services necessary for the critical function of cancer radiation therapy rather than simply disrupting the electronic health record systems and other, more traditional IT infrastructure," indicting that in some cases (at least in this case), the solution to the initial problem of "non-access" in a medical device context can lead to larger problems when traditional solutions are applied. This implies that a synthesized approach to both known/anticipated vulnerabilities and compatibility with commonly-used remediations and mitigations in the event of a cybersecurity event is an important consideration for medical device manufacturers.

John Ward – Cyberblog July 2021

The NIST is looking for a way of designating "critical software" within critical infrastructure. The FDA, in their response paper, states that in a healthcare context critical software is software that meets the definition of a "device" in section 201(h) of the FDCA (Food, Drug and Cosmetic Act-see reference list at the conclusion of this paper). For the FDA, software that does not meet the criteria of section 201(h), but where it is "necessary for the safe and effective use of a device" is also considered "critical software".

The FDA also agrees with the proposed SBOM standardization/guidelines from the NIST and Executive Order, which are largely in line with their views on SBOMs as mentioned above. Beyond SBOMs, the FDA is adamant about the importance of risk management, and indicate that they rely on AAMI TIR57, which is based on the IEEE paper "The Protection of Information in Computer Systems", and suggests that the NIST "consider this IEEE paper in thinking how to close the gap for OT cybersecurity in the federal government's use of critical software." In response to the NIST's question on guidelines for software integrity chains and provenance, the FDA points to their work with the NTIA's Multistakeholder work on SBOMs, which they have been involved in since its' inception, and would "strongly support NIST closely examining the NTIA work as part of their exploration of guidelines for software integrity chains provenance". The FDA also mentions the importance of vulnerability disclosure, and references the NIST to look at AAMI TIR97 and ISO/IEC: 29147: 2014, as they are the FDA's recognized documents for vulnerability disclosure.

The FDA is also adamant about threat modeling, which they believe is an important component of the NIST's query on initial minimum requirements for testing software code. The FDA points to their work, in coordination with MITRE and MDIC, in setting up "threat modeling bootcamps" (these bootcamps have been covered in depth by this author in previous reports to Ward Sciences and Consulting, and links will be provided at the conclusion of this paper). According to the FDA "Threat modeling helps to lay the groundwork for science-driven penetration testing and other downstream security testing". In this realm, the FDA insists on the importance of penetration testing, static and dynamic code analysis, and testing to failure rather than testing to "seems to work", are of paramount importance, as outlined both in AAMI TIR57 and Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2018).

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog July 2021

REFERENCES CITED AND RELATED CYBER RESOURCES OF INTEREST

1. Interview with Dr. Kevin Fu - https://www.medtechdive.com/news/FDA-cyber-chief-talks-medical-device-risks-agency-priorities/602625/

2. NTIA SBOM - https://www.ntia.gov/SBOM

3. NIST Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security- (https://www.fda.gov/media/149954/download)

4. Executive Order 14028 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

5. MDIC Threat Modeling https://mdic.org/project/medical-device-cybersecurity-threat-modeling/

6. US FDCA (see section 201(h) for the relevant portion on the definition of "device") https://www.fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act