WARD SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

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

John Ward – Cyberblog April 2023

RECENT CONGRESSIONAL LEGISLATION EXPANDS FDA AUTHORITY FOR CYBERSECURITY PREMARKET SUBMISSION REQUIREMENTS

A MOMENTOUS YEAR FOR MEDICAL DEVICE CYBERSECURITY

On April 7th of 2022 the FDA released *Draft Guidance: Cybersecurity in Medical Devices: Quality Systems Considerations and Content of Premarket Submissions*. This draft guidance greatly expanded on the recommendations that had been provided in a previous iteration released in 2018; that draft guidance had been released to supplement the original 2014 *Final Guidance: Content of Premarket Submissions for Management of Cybersecurity of Medical Devices*. In the past the release of a draft guidance would not have been particularly significant in the medical device regulatory landscape. Draft guidance documents offer medical device manufacturers (MDMs) insight into the FDA's current thinking on cybersecurity for medical devices but contain only non-binding recommendations. The 2022 premarket draft guidance contained comprehensive resources and recommendations for SBOMS, threat modeling, security risk management, a secure product development framework (SPDF), and total product lifecycle (TPLC) considerations, but MDMs were unlikely to receive a Refuse to Accept (RTA) on their premarket submission if they neglected to consider these recommendations.

AN IMPORTANT EXECUTIVE ORDER FOR IMPROVING THE NATION'S CYBERSECURITY

For the previous eight years MDM's were only beholden to the 2014 final premarket guidance and the 2016 *Final Guidance: Postmarket Management of Cybersecurity in Medical Devices* when submitting their 510(k)s. For stakeholders and observers in the medical device cybersecurity space it had been increasingly evident that significant regulatory changes were coming. The initial indication of this regulatory shift was the release of President Biden's *Executive Order on Improving the Nation's Cybersecurity (May 21st, 2021)*. While private industry was not directly affected by the content of this Executive Order (unless doing business with the federal government) it indicated a governmental focus on cybersecurity regulations and tasked the NTIA with publishing the minimum elements for an SBOM (Software Bill of Material). The FDA worked closely with the NTIA in the development of the minimum elements of an SBOM and the inclusion of an SBOM was a primary recommendation featured in the 2022 FDA premarket draft guidance.

EARLY 2022 LEGISLATIVE ACTION ON MEDICAL DEVICE CYBERSECURITY – THE PATCH ACT

In March of 2022 a bipartisan bill was known as the *Protecting Medical Devices from Cyber Attacks (PATCH) Act* was introduced to congress as a direct response to the proliferation of ransomware attacks in the healthcare sector. The purpose of the bill was to "implement critical cybersecurity requirements for manufacturers applying for premarket approval through the FDA", which was proposed to be facilitated through amending the Federal Food and Drug Cosmetic Act.

John Ward – Cyberblog April 2023

RECENT CONGRESSIONAL LEGISLATION EXPANDS FDA AUTHORITY FOR CYBERSECURITY PREMARKET SUBMISSION REQUIREMENTS

These proposed amendments would require MDMs to include SBOMs and a Coordinated Vulnerability Disclosure (CVD) process in their premarket submissions. The PATCH Act also sought to empower the Secretary of Health and Human Services to require that premarket submissions from MDMs require "…such information as the Secretary determines to be appropriate" regarding cybersecurity.

CONTINUED 2022 LEGISLATIVE ACTION ON MEDICAL DEVICE CYBERSECURITY

In May of 2022 another bipartisan medical device cybersecurity bill was introduced to Congress: the *Strengthening Cybersecurity for Medical Devices Act*. This act sought to require the FDA to regularly review and update their medical device cybersecurity guidelines and suggestions. The Act also empowered the federal Cybersecurity and Infrastructure Agency (CISA) to take an active role in reviewing and updating FDA medical device cybersecurity guidance documents and would formalize communication protocols and intervals between CISA, the FDA and the Secretary of HHS. The act also sought to require an update to 2022 premarket guidance that would upgrade it to "final guidance" status. The remaining portions of the act concerned the commissioning of a report by the Governmental Accountability Office to address challenges in healthcare cybersecurity communication, resources and communication as well as requiring the Secretary of HHS to update FDA-provided information to the public regarding medical device cybersecurity.

The status of both pieces of proposed legislation remained as "introduced" for the remainder of 2022. Their cause was bolstered in November 2022 when Senator Mark Warner (D-VA) released the policy paper *Cybersecurity is Patient Safety: Policy Options in the Health Sector* which addressed a wide range of cybersecurity concerns and policy ideas to address them. Suggested policies within Sen. Warner's paper regarding SBOMs, DHS/CISA coordination and information sharing with critical infrastructure entities and stakeholders and addressing insecure legacy systems were in-line with the spirit as well as the specificities of the proposed legislation and President Biden's Executive Order.

ENDING THE YEAR WITH A LEGISLATIVE AMENDMENT TO EXPAND FDA CYBERSECURITY OVERSIGHT

On December 29th, 2022, the Consolidated Appropriations Act 2023 ("Omnibus") was signed into law and codified the intent and many of the specificities of the previously mentioned Executive Order, proposed legislation, and policy paper into an amendment to the Federal Food and Drug Cosmetic Act, giving the FDA specific authority to enforce key cybersecurity requirements.

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

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

John Ward – Cyberblog April 2023

RECENT CONGRESSIONAL LEGISLATION EXPANDS FDA AUTHORITY FOR CYBERSECURITY PREMARKET SUBMISSION REQUIREMENTS

Sec 524B. *Ensuring Cybersecurity of Medical Devices* of the Omnibus Bill states that MDMs submitting a device for premarket approval **must include a vulnerability management plan including CVD, a postmarket update and patching plan, an SBOM and other criteria to provide "reasonable assurance that the device and related systems are cybersecure…**". The Omnibus also included the requirements for the GAO report, guidance revision and government/stakeholder communication as initially indicated in the proposed *Strengthening Cybersecurity for Medical Devices Act.*

HEADS UP FOR MEDICAL DEVICE MANUFACTURERS

The Omnibus bill mandated the effective date of these particular amendments as 90 days after the date of enactment. This means that as of March 29th, 2023, all premarket submissions to FDA by MDMs must include the criteria listed in section 524B(b) of the Bill, including the following:

- A plan to monitor, identify, and address, as appropriate, in a reasonable time, **postmarket** cybersecurity **vulnerabilities and exploits**, including **coordinated vulnerability disclosure** and related procedures;
- Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available **postmarket updates and patches** to the device and related systems to address—
  - on a **reasonably justified regular cycle, known unacceptable vulnerabilities**; and
  - as soon **as possible out of cycle, critical vulnerabilities** that could cause uncontrolled risks;
- Provide a **software bill of materials**, including commercial, open-source, and off-the-shelf software components;
- Comply with **such other requirements** as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

FDA TO THE RESCUE

On March 29th, 2023, the FDA released *Final Guidance: Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act*. The purpose of this short guidance was to inform MDMs that although the Omnibus amendments to the Federal Food and Drug Cosmetic Act are now in effect and enforceable, the FDA does not intend to issue RTA (Refuse to Accept) decisions to MDMs based "solely on information required by section 524B of the FD&C for submissions submitted before October 1st." The FDA intends to work collaboratively with sponsors of premarket submissions in this period "as part of the interactive and/or deficiency review process". On October 1st, 2023, the FDA may issue RTA premarket submissions that do not contain information required by section 524B.

John Ward – Cyberblog April 2023

RECENT CONGRESSIONAL LEGISLATION EXPANDS FDA AUTHORITY FOR CYBERSECURITY PREMARKET SUBMISSION REQUIREMENTS

This is a pivotal moment for MDMs to address cybersecurity governance, compliance, and resource allocation within their organizations. While one reading of the above guidance may indicate that MDMs can "kick the can" of 524B compliance until October 1st, they do so at the risk of delayed clearance or approval due to interactive review or even a hold letter with a list of deficiencies according to Naomi Schwartz, the senior director of Cybersecurity quality and safety at MedCrypt. Although the October 1st deadline only applies to a handful of specific submission requirements, it is evident from the Omnibus that further submission requirements will be compulsory in the near future with the mandated review and likely finalization of the most recent premarket draft guidance. A proactive approach to medical device cybersecurity compliance will likely be a key differentiator in successful/expedient 510(k) reviews and familiarization with the current premarket draft guidance will provide significant insight into the requirements, components and methodologies that have recently become or will rapidly become obligatory in the premarket submission process.

For this author's blog detailing the *Executive Order on Improving the Nation's Cybersecurity, the Patch Act* and the *Strengthening Cybersecurity for Medical Devices Act* please click here. For this author's blogs detailing SBOMs please click here and here.

Please contact John at jtward75@gmail.com for further information regarding FDA cybersecurity requirements. Ward Sciences and Consulting is available to help you with implementing a comprehensive premarket cybersecurity submission for your medical device software. We have recent and successful experience helping our clients with meeting these newly legislated medical device cybersecurity requirements.

