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 June 2022

SBOM RESOURCE LIST

Links to Current SBOM References, including Best Practices and Suggested Formats for SBOMs

SBOM RESOURCES

The FDA released the draft guidance *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff* on April 8th of 2022. This is an update to the previous draft guidance regarding cybersecurity in premarket submissions released by the FDA in October of 2018. Among the more significant changes in this current draft guidance is the addition of a "Software Bill of Materials (SBOM)" which replaces the previous versions' guidance for the inclusion of a "Cybersecurity Bill of Materials" (CBOM). Please note that the term "CBOM" no longer appears in the guidance with the release of the April 8, 2022 draft. Also note that FDA recently conducted an online webinar (June 14, 2022) on the above-mentioned draft Cybersecurity guidance - future Ward Sciences Blogs will provide more information regarding FDA comments on SBOMs, based on the FDA webinar presentation.

On May 12, 2021 the Biden administration issued *Executive Order 14028 Improving the Nation's Cybersecurity*. Subsection (j) of Section 10 defines an SBOM as a "formal record containing the details and supply chain relationships of various components used in building software" and likens an SBOM to "a list of ingredients on food packaging". The purpose of an SBOM is to allow for streamlined and comprehensive risk management and vulnerability scanning by all concerned stakeholders including manufacturers, buyers, and operators by allowing them to reference an accessible index of a vendor or developer's software, which can include "Off-the Shelf (OTS)", open-source, and/or proprietary components. Paragraph (vii) of subsection (e) of Section 4 called for the establishment of standards, procedures, or criteria by the Director of NIST in accordance with the heads of agencies they deem necessary for "providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on their website". The *Executive Order* also called for the publishing of minimum elements for an SBOM in paragraph (x) subsection (e) of Section 4.

Since 2018 the National Telecommunications and Information Administration (NTIA) has facilitated the "Multistakeholder Process on Software Component Transparency" to provide stakeholders a forum to formulate and establish an SBOM baseline. The FDA was involved in this forum early and prominently and played a significant role in providing feedback and suggestions that have shaped the federal government's development of standardized SBOM protocols. This resource list contains a number of governmental resources to assist medical device developers understand the current state of the SBOM landscape.

John Ward – Cyberblog June 2022

SBOM RESOURCE LINKS

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

2) Draft Guidance for Premarket Submissions (FDA, 2022)- https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

3) The Minimum Elements For a Software Bill of Materials (SBOM) https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

4) Software Bill of Materials Elements and Considerations (Federal Register/NTIA)- https://www.federalregister.gov/documents/2021/06/02/2021-11592/software-bill-of-materials-elements-and-considerations

5) CISA SBOM-A-RAMA (Two YouTube videos of a CISA-hosted public event held in late 2021 discussing SBOMs)- https://www.cisa.gov/cisa-sbom-rama

6) Software Bill of Materials-(Collection of YouTube videos produced by the NTIA regarding SBOMs)- https://www.youtube.com/playlist?list=PLO2lqCK7WyTDpVmcHsy6R2HWftFkUp6zG

7) NTIA's SBOM Resource Page- https://ntia.gov/SBOM

8) NTIA SBOM: Formats and Tooling: https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_formats_energy_brief_2021.pdf

9) NTIA SBOM FAQ: https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf

10) NTIA How To Guide for SBOM Generation: https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf

END OF BLOG – CHECK BACK OFTEN FOR OUR EXPANDED COVERAGE OF SBOMS AND RELATED CYBER TOPICS FOR MEDICAL DEVICE MANUFACTURERS

