

# Cybeats Reports on Approval of the U.S. Omnibus Appropriations Bill That Mandates SBOM for Medical Devices

Toronto, Ontario--(Newsfile Corp. - December 29, 2022) - **Cybeats Technologies Corp. (CSE: CYBT) ("Cybeats" or the "Company")** is pleased to provide comments further to the successful passing of the \$1.7 Trillion omnibus appropriations bill. This new bill enacts legal requirements for all medical device manufacturers to ensure their devices meet certain cybersecurity standards, including providing SBOMs to the FDA.

The omnibus bill requires the submission of a Software Bill of Materials (SBOM) to the FDA that includes all standard, open source, and critical software components of medical devices. Cybeats' *SBOM Studio* provides medical device manufacturers with the capability to efficiently manage SBOMs and their software vulnerabilities, as well as provides solutions for SBOM exchange with regulatory authorities such as the FDA. Cybeats recently announced commercial pilots<sup>1</sup> with Fortune 500 companies which include medical device manufacturers, who are proactively seeking SBOM management solutions in preparation for FDA regulations.

*"With our existing engagements with Fortune 500 medical device manufacturers, SBOM Studio addresses the specific needs of the medical device industry as required by the FDA. This new cybersecurity oversight by the FDA will accelerate the shift toward the use of the SBOM standard, and creates favourable tailwinds for SBOM Management solutions like Cybeats SBOM Studio," said Yoav Raiter, CEO, Cybeats. "Organizations are now tasked with the difficult need of managing and securely sending their valuable SBOMs and software assets to the FDA, which is precisely what SBOM Studio product does. We expect our market-ready product to see accelerating traction in the medical device marketplace where requirements to implement SBOM are not optional."*

The FDA seeks to have express authority to require premarket submissions that include evidence demonstrating the assurance of:

1. the device's safety and effectiveness for purposes of cybersecurity;
2. that marketed devices demonstrate a reasonable assurance of the device's safety; and effectiveness for purposes of cybersecurity;
3. that devices have the capability to be updated and patched in a timely manner;
4. **that manufacturers provide a device Software Bill of Materials (SBOM) with their devices so users know which components of their devices are or may be subject to cyber threats;**
5. and that device manufacturers publicly disclose when they learn of a cybersecurity vulnerability so users know when a device may be vulnerable, and to provide direction to users to reduce their risk.<sup>2</sup>

Regulations like these are aimed specifically at enhancing software supply chain security and the adoption of SBOMs, which is fueling a spike in SBOM interest globally. The 2023 FDA budget includes \$95 million USD in additional funding for which includes the development of a comprehensive cybersecurity program for medical devices, which will be used to hire additional staff to oversee regulations and develop greater cyber expertise within the devices program.<sup>3</sup>

The provisions in the omnibus bill lay out important guidance to ensure device manufacturers are prepared to identify and react to post-market software vulnerabilities in their products within 90 days. Additionally, new SBOM requirements will force vendors to determine if problems exist in the third-party components they leverage in their software. Medical device manufacturers can no longer ignore the risks

posed to patients by security risks in the software they use.

Given the increasing use of software in connected medical devices, the cybersecurity provisions included in the 2023 omnibus represent an important step forward in ensuring medical device safety and security. Even well-constructed software can contain highly impactful vulnerabilities that can affect the ability of software to function properly, and with the widespread use of third-party and open source software, medical device manufacturers may not even be aware of exploits that can impact patient care.

### **Cybeats SBOM Studio**

Cybeats' *SBOM Studio* was developed to support organizations in managing SBOMs, support SBOM distribution to clients, and provide a single pane of glass to cybersecurity vulnerabilities. *SBOM Studio* accelerates vulnerability management, reduces the cost of protection, and improves compliance. *SBOM Studio* is now suited for medical device companies and healthcare software consumers like hospitals, that rely on thousands of product software.

A software supply chain is composed of the components, libraries, tools, and processes used to develop, build, and publish a software artifact<sup>4</sup>. Software vendors often create products by assembling open source and commercial software components. Cybeats' SBOM Studio allows medical device manufacturers to collect SBOM from their vendors and build necessary SBOMs for the products which need submission to the FDA.<sup>5</sup>

### **About Cybeats**

Cybeats is a leading SBOM Management and software supply chain intelligence technology provider, helping organizations manage risk, meet compliance and secure software from procurement, development through operation. Our platform provides customers with deep visibility and universal transparency into their software supply chain, as a result enables them to increase operational efficiencies and revenue. Cybeats. Software Made Certain. Website: <https://cybeats.com>

**SUBSCRIBE:** For more information, or to subscribe to the Company's mail list, visit:

<https://www.cybeats.com/investors>

### **Contact:**

James Van Staveren  
Corporate Development  
Phone: 1-888-713-SBOM (7266)  
Email: [ir@cybeats.com](mailto:ir@cybeats.com)

### **Forward-looking Information Cautionary Statement**

Except for statements of historic fact, this news release contains certain "forward-looking information" within the meaning of applicable securities law. Forward-looking information is frequently characterized by words such as "plan", "expect", "project", "intend", "believe", "anticipate", "estimate" and other similar words, or statements that certain events or conditions "may" or "will" occur. Forward-looking statements are based on the opinions and estimates at the date the statements are made, and are subject to a variety of risks and uncertainties and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements including, but not limited to delays or uncertainties with regulatory approvals, including that of the CSE. There are uncertainties inherent in forward-looking information, including factors beyond the Company's control. There are no assurances that the commercialization plans for the technology described in this news release will come into effect on the terms or time frame described herein. The Company undertakes no obligation to update forward-looking information if circumstances or management's estimates or opinions should change except as required by law. The reader is cautioned not to place undue reliance on forward-looking statements. Under the parent company, Scryb Inc., company filings are available at [sedar.com](http://sedar.com).

<sup>1</sup> <https://www.cybeats.com/news/cybeats-provides-commercial-update-with-respect-to-several-ongoing-commercial-pilots-with-fortune-500-companies>

<sup>2</sup> <https://www.fda.gov/media/157192/download>

<sup>3</sup> <https://www.fda.gov/media/157193/download>

<sup>4</sup> [https://en.wikipedia.org/wiki/Software\\_supply\\_chain](https://en.wikipedia.org/wiki/Software_supply_chain)

<sup>5</sup> <https://www.cisa.gov/sbom>

To view the source version of this press release, please visit <https://www.newsfilecorp.com/release/149837>