U.S. Department of Defense Deploys Cybeats' Product for Critical Cybersecurity

Toronto, Ontario--(Newsfile Corp. - September 24, 2024) - **Cybeats Technologies Corp. (CSE: CYBT) (OTCQB: CYBCF) ("Cybeats" or the "Company"),** a global leader in software supply chain security, is pleased to announce that it has been enlisted by the U.S. Department of Defense to deploy its *SBOM Studio*[1] platform.

As part of this deployment, Cybeats' industry-leading software supply chain technology will be used by multiple components of the US military, including the U.S. Army and U.S. Naval Air Systems Command. This project further solidifies Cybeats' position as a trusted provider of cybersecurity solutions to the U.S. government, and brings Cybeats' Software Bill of Materials ("SBOM") management solution to three branches of the U.S. military. Cybeats enables organizations to manage third-party software risk and to more quickly respond to increasingly frequent software supply chain attacks. The Department of Defense 2025 budget request was for $850 billion USD.[2]

"Having worked extensively with U.S. forces throughout my military career, it is a profound honor to once again collaborate with the U.S. Department of Defense, the world's largest and most formidable defense organization," said **Justin Leger, CEO of Cybeats**. *"Together with the department, we are exploring the unique challenges of software supply chain security within a military setting. These pilots represent a significant step forward for both Cybeats and the U.S. DoD as we contribute to the broader mission of national security by addressing emerging cyber threats."*

The market for Cybeats' solutions has been propelled by Executive Order 14028, which outlined SBOM mandates and enhanced supply chain risk management across the U.S. government, including the Department of Defence. This includes assessment and rapid response to supply chain vulnerabilities, evaluate vendor products for security software development, maintain inventories of open source software, and persistently monitor for newly disclosed vulnerabilities and supply chain attacks.[3]

As the industry's first and leading software bill of materials (SBOM) manager, *SBOM Studio* will identify software supply chain risks in real time, track and manage software vulnerabilities, and help ensure compliance with Executive Order 14028. This marks Cybeats' second deployment with a major U.S. government agency, further solidifying Cybeats' role in national cybersecurity efforts. In the past year alone, more than 75% of software supply chains were exposed to cyberattacks -and 40% of organizations took a month or longer to recover.[4] With the key benefits of vulnerability monitoring, automated risk analysis, and regulatory compliance, *SBOM Studio* helps its clients achieve improved cybersecurity outcomes, serving a broad range of users in the software supply chain.[5]

The National Security Agency and the U.S. Department of Defense released its 2023 recommended best cyber practices report, where Cybeats' *SBOM Studio*[6] product is the only commercial service featured for managing SBOMs[7]. Learn more here about how Cybeats can help you to manage risk and meet evolving cyber regulatory requirements.

About Cybeats

Cybeats is a cybersecurity company providing Software Bill of Material (SBOM) management and software supply chain intelligence technology, helping organizations to manage risk, meet compliance requirements, and secure their software from procurement to development and operation. Our platform gives customers comprehensive visibility and transparency into their software supply chain, enabling them to improve operational efficiency and increase 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

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 products 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. Company filings are available at sedarplus.ca.

---

[1] https://www.cybeats.com/sbom-studio

[2] https://www.defense.gov/News/Releases/Release/Article/3703410/

[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[4] https://www.blackberry.com/us/en/company/newsroom/press-releases/2024/software-supply-chain-attack-have-increased-financial-and-reputational-impacts-on-companies-globally-new-blackberry-research-reveals

[5] https://www.cisa.gov/sbom

[6] https://www.cybeats.com/sbom-studio

[7] https://media.defense.gov/2023/Dec/11/2003355557/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20MANAGING%20OPEN%20SOURCE%20SOF

To view the source version of this press release, please visit https://www.newsfilecorp.com/release/224371