

Vigilant Ops Distills New SBOM Mandates as Medical Device Manufacturers Face Aggressive 90 Day Compliance Deadline

*\$1.7 Trillion Federal Spending Bill
Includes Stringent Medical Device
Cybersecurity Requirements*



PITTSBURGH, PA, USA, January 6, 2023

/EINPresswire.com/ -- On December

29, 2022, United States President Joe

Biden signed into law the \$1.7 trillion federal government spending package, officially avoiding a government shutdown. "What this means for the Medical Device Manufacturer community is that FDA now has legal authority to require specific cybersecurity related documentation starting 90 days from the signing of the bill. By (or before) the end of March 2023, they must be prepared to submit specific documentation." said Ken Zalevsky, CEO at [Vigilant Ops](#).

Specific documents include:

- Software Bill of Materials including commercial, open-source, and off-the-shelf software components
- Vulnerability monitoring plans addressing postmarket cybersecurity vulnerabilities and exploits
- Postmarket cybersecurity updates and patches periodically and on-demand

A particularly burdensome requirement for medical device manufacturers is the secure maintenance and monitoring of devices at customer sites. The continuous monitoring of vulnerabilities and the need to respond with security patches on a "...reasonably justified regular cycle..." and "...as soon as possible out of cycle..." means that informal, manual solutions will not be sufficient to meet the letter of the law.

Vigilant Ops has been at the forefront of these looming requirements, offering a cost-effective solution immediately available to medical device manufacturers of all sizes. "We founded Vigilant Ops with the healthcare industry in mind and have leveraged our collective global medtech experience to develop the [InSight Platform](#), the leading SBOM generation, management, and vulnerability monitoring tool on the market today," said Zalevsky. "Our InSight Platform is already being utilized at some of the world's largest medical device manufacturers, and we are continuing our intense focus on solution development and innovation as the SBOM ecosystem

continually evolves.”

Vigilant Ops has closely monitored the US Food and Drug Administration lobbying efforts focused on similar requirements since their initial draft of “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices” issued on October 18, 2018. We have followed the progression of FDA requirements to ensure that Vigilant Ops cybersecurity solutions meet or exceed the expected standards. As far back as September 2021, we reviewed FDA’s request for legislative authority to enforce the requirement of a Software Bill of Materials and vulnerability monitoring plan.

Securing the Software Supply Chain

In addition to SBOM generation, continuous vulnerability monitoring, and sophisticated SBOM management, the InSight Platform leverages natural language processing techniques and patent-pending machine learning algorithms to efficiently and effectively find vulnerabilities associated with device components, eliminating false positives, and making an impossible task reliable, scalable, and automatic.

In Summary

The US government has long been concerned with the improvement of the nation’s cybersecurity posture, and this recently passed legislation is the culmination of years of effort and various legislative and guidance documents including the [Presidential Executive Order 14028](#), released in May 2021. In response to the continuing threats and attacks in healthcare, the bill details the new legal requirements that must be met by all medical device manufacturers to ensure the cybersecurity of their products. Medical device manufacturers still trying to manage the effort in-house will end up having to divert an enormous quantity of resources to the issue, possibly slowing innovation and product development. The passage of this bill into law, however, will precipitate a sea change in the cybersecurity posture of medical device manufacturers. Complying with the law might be the immediate concern but lacking the ability to deliver on required cybersecurity mandates will quickly lead to further speculation from customers and lost opportunities and revenue.

About Vigilant Ops

Founded in 2019, Vigilant Ops is an innovator in the medical device cybersecurity industry. Led by medical device cybersecurity experts with more than forty years of combined experience, Vigilant Ops provides medical device manufacturers and hospitals with unprecedented insight into device risk profiles, enabling compliance with cybersecurity laws and proactive management of threats, before they impact the quality of patient care.

Learn More

For more information or to demo/trial the InSight Platform, please visit us at <https://www.vigilant-ops.com>

Alicia Bond
Vigilant Ops, Inc.
+1 412-704-4585

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/609787021>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.