

3 Takeaways on What The Omnibus Bill Means for Medical Device Manufacturers

The below piece is based on the resource: [How FDA and the Omnibus Bill Will Reshape Pre & Post Market Product Security](#)

The December 2022 Omnibus bill, a large spending bill passed by the US government, continues the Biden administration's rhetoric of securing America's infrastructure.

Buried within this bill are new powers granted to the Food and Drug Administration, allowing them to double down on medical device product security and turn previous guidelines into new regulation. However, the ecosystem now finds itself in a limbo period where we can only speculate on which guidelines will become requirements, and which will fall to the waist side.

Looking at interviews, first-hand research, attack trends on medical facilities, data collected from primary sources, publications, and [regulations](#), we put together a resource on [how the FDA and Omnibus bill will reshape product security](#).

Here are our three main takeaways:

1. What will be the FDA's approach to security?

Before we can speculate on what the future regulation will require of MDMs and medical facilities, it's important to understand what will drive future pre and post market regulations.

After speaking with Dr. Schwartz, Director, Office of Strategic Partnerships & Technology Innovation, Center for Devices & Radiological Health, US FDA, the very leader of this charge towards securing these mission-critical devices, we noted that her focus will be what has worked time and time again– trustworthiness, transparency, and resilience.

"[Resilience] really gets at the heart of the legacy challenge that we face today. With so many devices on the market, in spite of being able to identify vulnerabilities in them, they can't be patched," said Dr. Schwartz regarding what we can learn from the past. "They should be updateable and they should be able to perform in the way that they were intended while receiving updates and fixes in real time."

Trustworthiness, transparency, and resilience are only possible when you know exactly what it is that you are trying to make resilient. With large component libraries filled with variations from new, third-party, open source, and custom open source code, many companies must sheepishly admit that they don't actually know every piece of software that exists in their products.

To address this alarming reality, manufacturers can expect strict regulations surrounding documentation, management, and distribution of software bills of material (SBOMs)-- giving teams clear visibility into what software components exist within each device.

2. Post Market considerations, to consider during development

Some of the [latest regulations](#) put out by the FDA go back as far as 2016. While guidelines have been updated as recently as last year, requiring manufacturers to not only follow today's regulations but be prepared for whatever may come next.

In this case, MDMs need to see post market considerations as foreshadowing, demanding that they [shift-right](#) for full lifecycle product security.

This can be achieved through [proper SBOM generation and management](#) from the beginning of development through the full lifetime of a product. When managed well, SBOMs allow product security professionals to understand each software component within a device and apply patches, roll out updates, and conduct vulnerability management activities at scale.

3. Remediation and reporting

Considering the staggering number of cyber attacks on medical facilities, product security pros are doing all they can to ensure that their device doesn't become a vulnerable endpoint.

However, it is still critical to know what to do, should a breach occur.

If a patch is needed to remediate a newly discovered vulnerability, there is no need to run it by the FDA or re-apply for approval, as long as the patch means that the patient's level of protection remains the same as the initial submission previous regulations state "These types of changes are not to reduce uncontrolled risk of patient harm, and therefore not to reduce a risk to health or to correct a violation of the FD&C Act. They include any regularly scheduled security updates or patches to a device, including upgrades to the software, firmware, programmable logic, hardware, or security of a device to increase device security, as well as updates or patches to address vulnerabilities associated with controlled risk performed earlier than their regularly scheduled deployment cycle even if they are distributed to multiple units." But, medical device manufacturers have to consider that once a vulnerability is discovered the clock starts ticking. "FDA encourages efficient, timely and ongoing cybersecurity risk management for marketed devices by manufacturers."

SBOMs as a foundation for cyber compliance

While in the past these postmarket guidelines weren't enforceable, and they still are considered 'guidelines', it seems that there is enough evidence to draw a conclusion: These guidelines will soon become requirements.

But just generating SBOMs is not enough, as it will leave you with an endless list that cannot be managed or used for discovering and remediating critical vulnerabilities at scale.

To break it down, SBOMs are the launchpad for:

- **Security:** Knowing the specific versions of software used in a medical device can help identify vulnerabilities that may exist in older versions. This information can be used to patch or upgrade the software to address any known security issues.
- **Compliance:** SBOMs can help medical device manufacturers demonstrate compliance with regulations such as the FDA's Software as a Medical Device ([SaMD](#)) guidance, which requires manufacturers to maintain a record of the software components used in their devices.
- **Supply Chain Management:** SBOMs can help medical device manufacturers understand their supply chain and identify any potential risks. For example, if a component used in a medical device is discovered to have a security vulnerability, the manufacturer can use the SBOM to identify which devices may be affected and take appropriate action to address the issue.
- **Traceability:** SBOMs can also help medical device manufacturers trace the origins of a specific component, which can be useful in case of a recall.

The list of benefits go on but overall, SBOMs play a critical role in ensuring the security, safety, and compliance of medical devices, and in providing supply chain transparency and traceability.

Visibility demands management

SBOMs on their own hold a trove of actionable information, but only if they can be managed properly.

Cybellum's Product Security Platform helps companies use these lists of software ingredients to increase transparency, bolster vulnerability management, and quickly respond to incidents thanks to actually knowing each component that exists in a device. Going beyond SBOM generation to management, some companies choose to directly integrate the platform into existing workflows, allowing teams to access the most up to date information, with a custom SBOM for each device.

This leads to faster time to cyber compliance and policy management across devices, business units, and the entire organization.

Read: [How FDA and the Omnibus Bill Will Reshape Pre & Post Market Product Security](#)