

How the FDA and the
Omnibus Bill Will Reshape

PRE & POST MARKET PRODUCT SECURITY



TABLE OF CONTENTS

Preface

Medical cybersecurity's seismic shift

What will be the FDA's approach to security?

Post Market considerations, to consider during development

Monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle

Design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to Off-the-shelf software

Establishing and communicating processes for vulnerability intake and handling

Remediation and reporting of cybersecurity vulnerabilities

Here come the SBOMs

So, what are medical device manufacturers expected to change?

Cybellum, where teams do product security

SBOM

Vulnerability Management

Compliance Management

Product Incident Response (PSIRT)

And Managers can manage it all in one place

About Cybellum

Preface

A Chief Product Security Officer (CPSO) is expected to flawlessly orchestrate a symphony of cybersecurity protocols and requirements, keeping business units, their devices, and the people who rely on them completely safe. But, one wrong note, and the performance quickly turns to chaos and worry of recalls.

One piece of vulnerable supply chain software component;

One line of code in [custom OSS](#) that didn't define injection parameters;

One legacy device improperly configured with a modern one that creates a vulnerable gateway into the network.

Make no mistake- this fight is not fair.

To the frustration of US regulators, hackers have proven to remain one step ahead of legislated requirements by finding a weakness further downstream, in the software supply chain. To address this, December 2022's Omnibus bill grants the FDA powers to reign in a vast landscape of medical devices that can wreak havoc on patient care with a single breach. This demands better premarket through post-market cybersecurity stringency along with product-security focused solutions that can enable continuous security maintenance at scale.

At the heart of any selected tool or process must be SBOM management, allowing for companies to share the most up-to-date components list with product owners. This will guide premarket activities and allow companies to prevent recalls that result from improperly-secured connected devices.

Below, we combined the realities of cybersecurity attacks on medical facilities, data collected from primary sources, and [first-hand research](#), interviews, publications, and [regulations](#).

We invite you to read below and start a conversation with your peers about what medical device security will look like in 10 years from now if we take action today.



Medical cybersecurity's seismic shift

The varied nature of Product Security means that a one-size-fits-all protocol has eluded us. Without an agreed up on framework, every company conducts their own market research and threat intelligence to measure which way the cybersecurity wind blows. "Is this still the best practice? Will it really protect me against a committed hacker?" are just day to day considerations for today's medical device manufacturer's cybersecurity leadership.

As the Biden administration shows no sign of slowing down their mission to cyber-secure the country's supply chains, infrastructure and devices we rely on, there is no doubt that a new level of oversight can be expected from the Food and Drug Administration (FDA) with SBOMs at it's core. In the December 2022 Omnibus bill, the FDA has been granted the resources for tighter oversight and cyber compliance for medical devices, which have become increasingly connected and a target of choice to penetrate healthcare facilities.

Below are a few questions we try to answer for those preparing themselves to tame the treacherous seas that is medical device cybersecurity in 2023. In today's waters, not considering compliance guidelines during development can risk time to market delays, recalls or market removal tomorrow.

What will be the FDA's approach to security?

Less than 12 months ago an alarming amount of healthcare leaders said they weren't adequately prepared for a cybersecurity attack on their facility. According to the [2022 Medical Device Cybersecurity Survey](#), "Almost all respondents believe they are at least partially ready for a cyber-attack, and 75% believe they are better prepared than the competition. Despite this self-confidence, the truth is that 65% of companies noted that they only test their device firmware at most once a month, and more than a third (34%) say that incident response is an exposed area for them in device security."

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 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." This sentiment echoes throughout FDA document as it continuously reminds the reader that an update or security patch is part of normal use and alone does not constitute a new release that needs FDA re-review (more details below under 'Remediation and reporting of cybersecurity vulnerabilities').

This has been clear since the earlier days of medical device cybersecurity awareness. "[Our team has] seen a fair amount of examples with respect to how an impact on a medical device can certainly affect its function in ways that either it doesn't function at all or it functions inappropriately. That has the potential to be lethal at the worst, or at least damaging to patients," said Dr. Schwartz. "So, we had to face reality. As has always been the case, we're not waiting for that first death or injury to occur in order to take action." Even if not fatal, many of today's attacks lead to leaked patient personal information- causing them great distress at no fault of their own.

Combining her insight with the FDA's 2022 premarket guidelines and 2016's [Postmarket Management of Cybersecurity in Medical Devices- Guidance for Industry and Food and Drug Administration Staff](#), along with greater oversight powers, can help medical device manufacturers understand how today's sentiments, such as were discussed with [Dr. Schwartz on the Left to Our Own Devices podcast](#), will translate into tomorrow's FDA standards. This is lock-step with the CISA who is also determined to see SBOMs used widely across industries. Their website states "CISA will advance the SBOM work by facilitating community engagement, development, and progress, with a focus on scaling and operationalization, as well as tools, new technologies, and new use cases. This website will also be a nexus for the broader set of SBOM resources across the digital ecosystem and around the world."

Post Market considerations, to consider during development

Pulling no punches, this document states on page 13, under Postmarket Considerations, *“It is essential that manufacturers implement comprehensive cybersecurity risk management programs and documentation consistent with the Quality System Regulation, including but not limited to complaint handling, quality audit, corrective and preventive action, software validation and risk analysis and servicing.”*

It then continues to outline what actions would be needed to satisfy these guidelines. To start, manufacturers must maintain a robust software lifecycle processes that include mechanisms for:

Monitoring third party software components for new vulnerabilities throughout the device’s total product lifecycle

By today’s standards, achieving this is only possible with proper SBOM management, a list of all of the components and dependencies that make up a specific piece of software. It includes information such as version numbers, authors, and licenses for each component, and can be used for security, compliance, and supply chain management purposes.

Modern tools can automate this process, generating SPDX, CycloneDX, SWID or other formatted SBOM reports.

Once these are organized, it paves the way for better observance of premarket guidelines, post market necessities, [Vulnerability Exploitability eXchange \(VEX\)](#) reports, vulnerability management, and lots more.

Even more critical, it standardizes how organizations can communicate newly discovered vulnerabilities and possible mitigation steps rapidly, as noted on page 14, *“It is strongly recommended that manufacturers participate in an ISAO that shares vulnerabilities and threats that impact medical devices.”*

This is important considering that each product may contain tens of components and SBOMs. From there, each product has multiple versions based on varying factors, and finally, there can be tens or hundred of products. This can lead to an avalanche of bills of material that must be managed on an ongoing basis, ensuring that what’s listed on an SBOM is always up to date.

Design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to Off-the-shelf software

Make sure that before deploying updates not only do you remediate the discovered vulnerability but also don’t change the level of risk faced by a patient or facility using it.

This can be especially tricky when vulnerabilities are introduced earlier in the supply chain, by the development team’s own submissions, or when using Custom Open Source Software who’s vulnerability management responsibilities fell between the cracks. Ronen Lago, former head of security at Daimler AG, Lockheed Martin, and current Board Member at Cybellum, said *“Cherry-picking from two safe open source packages may save time but by chiseling out the pieces that are most relevant, developers are inherently foregoing the protections that come from reliable open source libraries.”* He continues, *“Key questions about who is responsible for the ongoing monitoring, patching, and security needs of the product all have one simple answer: no one. Unless a clear agreement is reached between organizations and their vendors about who will maintain the software over time, companies must take full responsibility for securing their products, along with the custom open source software they rely on.”*

Establishing and communicating processes for vulnerability intake and handling

It’s one thing to be able to communicate vulnerabilities and discover remediations, but how is that information shared with stakeholders, including medical facilities and individuals who have some of these machines operating in private residences?

From the very beginning of development, SBOMs must be generated and managed to obtain the most up-to-date information regarding the products software “ingredients”. Throughout the development and compliance stages, these documents should be shared alongside relevant vulnerability exploitability exchange (VEX) reports- informing the purchaser of known cybersecurity vulnerabilities within their specific product and framework.

A process must be established for the proper intake, prioritization, and mitigation of any vulnerability that is discovered, both during development and throughout the full lifecycle of the device. On page 15 under Medical Device Cybersecurity Risk Management, it states “Manufacturers should have a defined process to systematically conduct a risk evaluation and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk.”

With compliance demands already requiring SBOMs, companies should use them as a guide for empowering their product security incident response team ([PSIRT](#)).

These teams, made up of cross-disciplinary members are designed to jointly orchestrate internal and external facing activities in relation to incident response, allowing for better control and response time towards an unexpected product security scenario event. By assigning the vulnerability to the most relevant member, it can be prioritized and addressed quicker. What’s more, the point of contact in the future is the person who is best suited to address any follow-up questions.

Remediation and reporting of cybersecurity vulnerabilities

Throughout the development, testing, and even deployment process, companies must consider the inevitable question: “What do I tell the FDA if one of those dreaded risks are found?”

First consider, what is a patch and what is considered a new version. On page 9, under Cyber Routine Updates and Patches, it explains that if issuing a patch means that the patient’s level of protection remains the same as the initial submission: “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. Page 18, under Remediating and Reporting Cybersecurity Vulnerabilities, says “FDA encourages efficient, timely and ongoing cybersecurity risk management for marketed devices by manufacturers.”

If you are unsure if what you have is a patch then it must fall within this explanation: “Changes to a device that are made solely to strengthen cybersecurity are typically considered device enhancements, which may include cybersecurity routine updates and patches, and are generally not required to be reported, under 21 CFR part 806. Even when risks are controlled, manufacturers may wish to deploy an additional control(s) as part of a ‘defense-in-depth’ strategy. Typically, these changes would be considered a cybersecurity routine update or patch, a type of device enhancement; Device changes made solely to address a vulnerability that, if exploited, could lead to compromise of PHI, would typically be considered a cybersecurity routine update or patch;”

To summarize, for ongoing post-market review, it will be expected that companies:

- Adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the initial vulnerability report to the vulnerability submitter
- Proactively practice good cyber hygiene, reassess risk assessments regularly, and seek opportunities to reduce cybersecurity risks even when residual risk is acceptable;
- Conduct appropriate software validation under 21 CFR 820.30(g) to assure that any implemented remediation effectively mitigates the target vulnerability without unintentionally creating exposure to other risks;
- Provide users with relevant information on recommended device and compensating controls and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use
- Recognize that some changes made to strengthen device security might also significantly affect other device functionality (e.g., use of a different operating system) and assess the scope of change to determine if additional premarket or postmarket regulatory actions are appropriate.

Here come the SBOMs

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.

This is not a shock but a wakeup call. The kind that has you jump out of bed in a full sprint.

This is one of those times that 'postmarket' should be seen as foreshadowing, [shifting critical cybersecurity practices left](#) and ensuring that security is a top priority from ideation through FDA submission and beyond.

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.

So, what are medical device manufacturers expected to change?

What internal process will medical device manufacturers be expected to revamp? That depends on how closely they've been following the guidelines and if product's have taken a future-proofing approach from early on in the development lifecycle.

While some may say that keeping to these guidelines were a bit like playing hide and seek up until now, it's time to put everything out in the open- with benefits that go well beyond faster time to compliance and mitigating delay risks. Organizations who are prepared to share their security-related information will find themselves thriving at a time when purchasers want to see SBOMs as a precondition for coming to the table. If you can rapidly call upon approved SBOM, VEX, and the relevant compliance information when others are still struggling to understand what's in their devices, it sends a clear message- your brand is ready to do business.

In the new world of medical device cybersecurity, brand reputation will not be measured by number of units sold but by the proactive approach taken to securing healthcare facilities and the patients that rely on them to remain healthy.



Cybellum, where teams do product security

Above trying to understand and manage all of the premarket guidelines, postmarket requirements, executive orders, and industry-specific standards, someone has to actually manage and oversee all aspects. To reduce pressure on security teams and enable them to perform tasks that are already nearly impossible to manage at scale, a dedicated product security solution is required.

SBOM Management

To comply with internal and external policies, SBOMs need to be verified, tracked, and approved for each product, component, and version, across multiple teams including development, QA, compliance, and of course security....

Cybellum automates the entire SBOM management process, so you go from detection to approval and vulnerability management in no time.



Manage all SBOMs in one place - Gain deep visibility into your supply chain, 3rd party software components, and proprietary code across components, products, and business units.



Track SBOM versions through time - Create and manage SBOMs continuously with every new version, and see the changes through time.



Make compliance much easier - Create, validate and generate reports quickly, so you easily meet industry standards from the likes of the FDA, ISO and others.



Integrate SBOM generation into existing workflows - Seamless integrations with your existing system such as PLM, CI/CD, and software update systems, and support for all SBOM and VEX format, such as CycloneDX and SPDX, including import and export.



Beyond simple SBOMs - Expose all associated risks beyond the simple SBOM, such as HW BOM, cryptography, passwords, PII, OS configuration, and more.



Focus more on security research, less on SBOM validation - without the costly and time consuming hassle of manual audits, you will be able to focus your time where it counts, on reducing risk and remediating critical vulnerabilities.

Vulnerability Management

Understand the real risk impact. Cybellum analyzes your device software in incredible detail, then matches it with a dedicated product vulnerability database. Clearly understand which vulnerabilities pose an immediate threat to your products and which ones less so.



Noise Cancellation - Reduce the noise caused by false positive and low-priority risks with a platform that removes manual vulnerability prioritization.



Industry Focused - Whether in the automotive, medical device, or industrial sector, each field has a unique ecosystem. Gain contextualized insights based on Cybellum's industry specific solutions to better prioritize vulnerabilities and regulatory demands.



Close the loop, from SBOM to Mitigation - Automate SBOM management, VEX generation, and mitigation orchestration, so you get from found to fixed in no time.



Continuous Post Production Assessments - Analyze and mitigate new software updates down the line.



Rapid Compliance with Cybersecurity Regulations - Meet new and existing regulations from ISO and the FDA, amongst many others.

Compliance Management

Automate the entire cyber compliance process. Rapidly identify cyber compliance gaps by matching pre-mapped regulatory requirements with vulnerability assessments, all automatically. Better visibility allows you to generate regulator-ready reports in only a few clicks.



Document - Keep a register of all evidence and relevant regulatory data for historical and auditing purposes, across all product lines and business units.



Stay on top of new standards - Keep up with new and existing regulations, standards and best practices such as the FDA Premarket Guidance, IMDRF cybersecurity practices, the European MDCG guidance, and others, by automatically integrating these policies into your workflow.



Comply faster and get certified - Automated regulatory validation highlights violations and delivers auto-compiled reports, allowing you to see what remains open, then generate detailed reports that perfectly match each standard's structure.



Comply at scale - Ramp up and improve compliance oversight and approval across products and teams.



Easily govern internal policies - Automate internal policy validation using the same engine to make sure all products comply with both internal and external requirements.

Product Incident Response (PSIRT)

Go from detection to investigation under one roof. See your most relevant risks to their post-production products, then facilitate detailed investigations - all in one central location.



Automate PSIRT grunt work so you could focus on thorough investigations - Quickly clear through noise and identify your products' most urgent vulnerabilities. Integrate seamlessly with your SIEM, SOAR and other operational systems, so you can quickly mitigate incidents.



Keep your finger on the pulse of all security-related events - Take decisive steps against the most relevant cyber risks, all in the context of your specific products and systems. Slash time to remediation and take critical steps towards keeping post-production products continuously secure.



Automate threat intelligence - Automated aggregation and monitoring of threat intelligence sources identify what's relevant to your specific products.



Facilitate entire investigations - Get a workbench for creating and managing investigations, from comprising relevant info, to formulating the analysis, and opening relevant tickets. Then, generate customized reports for each individual stakeholder.



Reduce remediation times - Leveraging pre-existing data about your product's software you can save time during threat monitoring and investigations and mitigate threats significantly quicker.



Comply faster with post production standards - Ensure post-production security to meet required industry standards, such as the FDA Post Market Guidance.

And Managers can manage it all in one place

Your most pressing issues, ready for action. The most important and impactful insights are waiting for you, allowing you to discover the most widespread vulnerabilities that affect many of your products, uncover the biggest compliance violations faced right now and even identify the riskiest supplier.



See trends over time - Track progress over time such as the percentage of products at risk, SLA tickets met, average resolution times, and more.



Achieve unprecedented control over your supply chain - See exactly which risks are coming from which supplier or vendor, pinpointing the riskiest components or suppliers.



Gain insights from every angle - Highlight the most crucial security risks, compliance gaps, and licensing challenges at any given moment.



Have full lifecycle visibility - Identify how many products you have at each lifecycle stage, then zero in on their security posture.



Quantify the progress - Put KPIs to product security activities and measure department ROI.



ABOUT CYBELLUM

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Leading manufacturers such as Jaguar Land Rover, Supermicro, Siemens, and Faurecia use Cybellum's Product Security Platform to execute and manage the main aspects of their cybersecurity operations across teams, product lines, and business units. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Powered by Cyber Digital Twins™ technology, Cybellum creates a live digital replica of every software component inside your devices, allowing product security teams to manage cyber risk continuously.



TO LEARN MORE VISIT WWW.CYBELLUM.COM



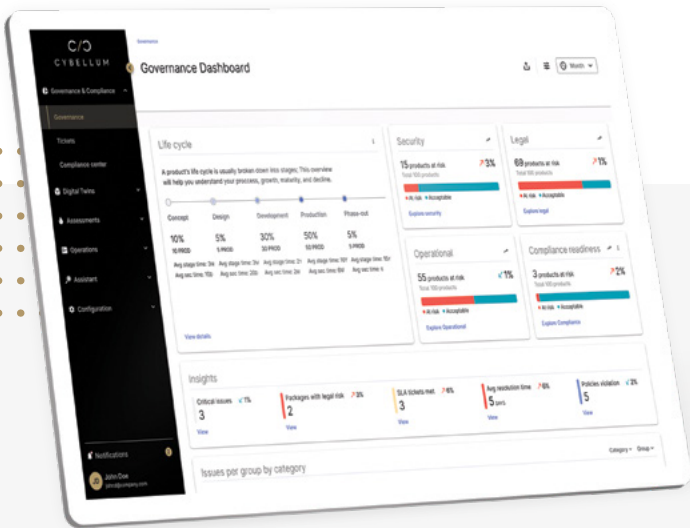
RESOURCE CENTER



PODCAST

LEARN MORE ABOUT PRODUCT SECURITY

BLOG



MORE ABOUT The Product Security Platform

FOLLOW US FOR NEWS AND UPDATES CYBELLUM.COM

