CYBELLUM

Safety First: Breaking Down the FDA's 2023 Premarket Cybersecurity Requirements

Table of Contents

This time, *it's for real*

The September 2023 release of the FDA's guidelines on pre market authorization and cybersecurity shows us that in a way, everything old is new again.

However, that doesn't mean it's exactly the same as it was. For many product security professionals, the changes between the 2022 draft and the 2023 publication don't set off alarm bells– and for others, the updates even bring a wave of relief.

While there is work to be done, these guidelines give clearer guidance and benchmarked points for professionals to measure their current activities against. For companies who are already managing SBOMs and automating their vulnerability detection and prioritization activities from a single centralized location, they can now see how their activities line up against the FDA's final guidelines.

For those who are still on their journey towards a more mature product security operation, these benchmarks present opportunities. It allows for operations to be realigned in one location instead of a patchwork of tools so the full product security journey can be conducted harmoniously and automatically. Teams can sharpen communication with end users, boost product security, ensure quality, check interoperability capabilities, and manage a device's full lifecycle.

So what really sets the 2022 and 2023 documents apart? The Omnibus.

Following the passing of the December 2022 Omnibus bill, the FDA has been granted the legal authority to require cybersecurity measures be placed on all marketed medical devices. This reflects the interest of the FDA in protecting patients, stating "For applications currently pending with FDA at the time of initial publication of this guidance, as well as those submitted after initial publication of this guidance, FDA intends to work collaboratively with manufacturers of such premarket submissions as part of the FDA review process."

But make no mistake, SBOMs will be customer facing, product security will be embedded in each part of the device, and only those who follow high security standards will be allowed on the market.

If you've been holding out on your product security activities, your time is now.

Does your device apply?

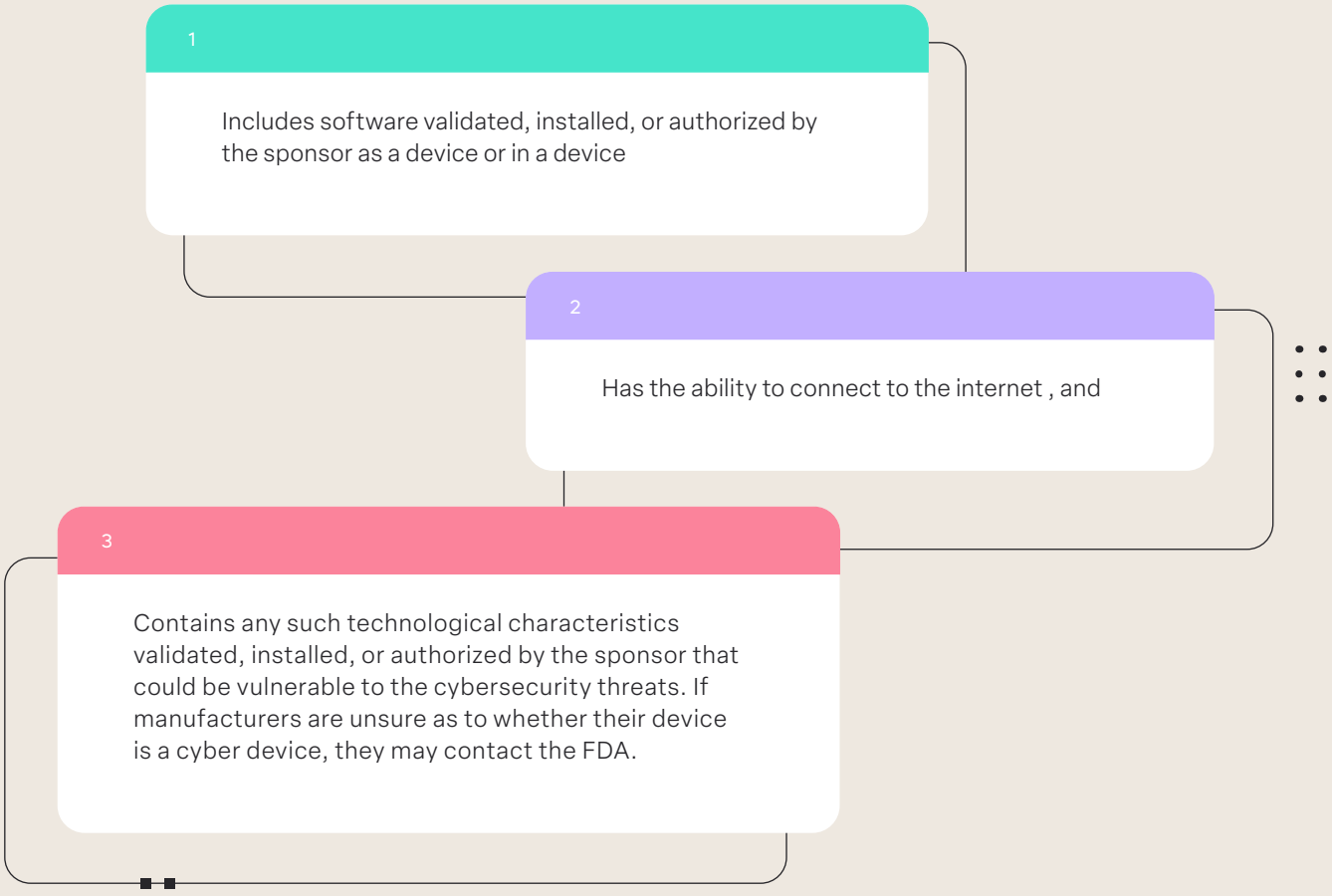
The U.S. Food and Drug Administration (FDA) defines a "cyber device" as a medical device that either incorporates software as a component or relies on software for its proper functioning.

The FDA's definition places paramount importance on cybersecurity within the medical technology development process– a necessity many medical facilities know too well as unsecure devices act as potential avenues for threat actors to impact patient care.

To ensure that appropriate regulations and safeguards are in place to protect your device and patient data, consider:

What is a connected medical device or 'cyber device'?

Section 524B(c) of the FD&C Act defines "cyber device" as a device that:

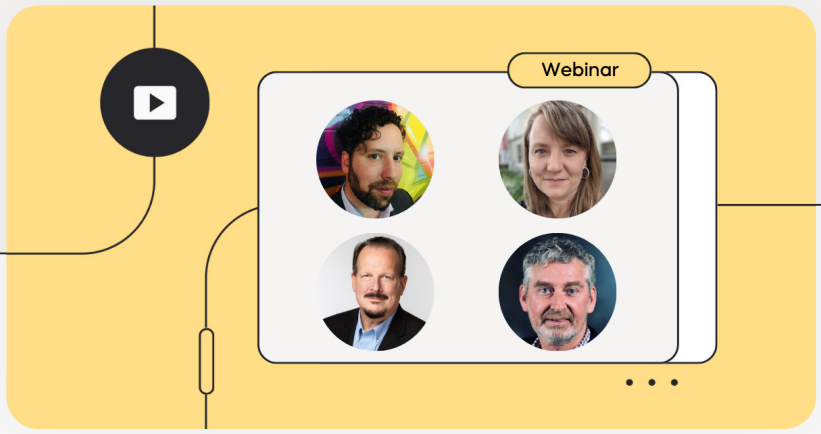


Is your product software defined or driven?

The FDA's cybersecurity requirements apply when a medical device is software-reliant, irrespective of whether the software is developed in-house by the manufacturer or sourced from a third party. This regulation is essential to guarantee that patient safety is upheld and critical healthcare data remains secure.

Does your device connect to the internet or to other internet-connected products?

Devices that rely on hard connections for connectivity, such as USB, SD, CD, ethernet cable, and others or wireless connectivity via Wi-Fi, Bluetooth, RF, cellular or other, are more susceptible to cybersecurity risks. Robust security measures are imperative to mitigate vulnerabilities associated with these interfaces.



Navigating the Future of Medical Device Security in the Evolving Regulatory Climate

The FDA's definition of a "cyber device" underscores the critical role of cybersecurity in the domain of medical technology. By emphasizing these considerations, the FDA aims to ensure patient safety and the integrity of healthcare data in an interconnected and technology-driven healthcare environment. This definition is a fundamental step towards maintaining the highest standards of security and safety within the rapidly evolving field of medical technology. The FDA's definition of a "cyber device" underscores the critical role of cybersecurity in the domain of medical technology. By emphasizing these considerations, the FDA aims to ensure patient safety and the integrity of healthcare data in an interconnected and technology-driven healthcare environment. This definition is a fundamental step towards maintaining the highest standards of security and safety within the rapidly evolving field of medical technology.

Security, safety, and quality are one and the same

The FDA views security, safety, and quality as a given for any medical device that can be marketed.

Bringing together security and quality is nothing new. In fact, we've seen this echoed in earlier drafts since unsecured devices operating in our facilities create a direct threat to hospitals, healthcare organizations, and patient health.

This document makes clear, "Cybersecurity threats to the healthcare sector have become more frequent and more severe, carrying increased potential for clinical impact. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the U.S. and globally. Such cyber attacks and exploits may lead to patient harm as a result of clinical hazards, such as delay in diagnosis and/or treatment."

> ***What we've seen is that when a hospital is hit by a ransomware incident, that's a patient safety issue. That's a public health issue.***
>
> **Jessica Wilkerson** | Senior Cyber Policy Adviser and Medical Device Cybersecurity Team Lead, FDA

This demand that companies review their components' security with a fine comb also presents an opportunity for quality teams to ensure that all functions are working properly and no piece of their product is left untested. This is especially true for medical devices that operate as their own internal system, relying on dozens of software components to conduct tasks. A weakness in one, whether it be poor design (quality) or security is a threat to an entire HDO as well as patient safety.

Ecosystem effort

Achieving secure activity across medical devices isn't achievable by holding a select group of manufacturers, vendors, or healthcare facilities responsible. Instead, it takes an ecosystem view where all stakeholders communicate with one another, sharing their challenges, identifying risk, and creating more secure processes—together.

> ***FDA recognizes that medical device cybersecurity is a shared responsibility among stakeholders throughout the use environment of the medical device system, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices.***
>
> FDA PMA 2023

A closer look at execution

Devices should be created with security in mind at all times.

Bringing cybersecurity into the fold is not a new concept. However, the FDA is giving teams specific considerations for when implementing a security-first approach, such as by leveraging Secure Product Development Framework (SPDF) and improving transparency.

Product security professionals should rely on SBOMs to expose all software components, frameworks, and secure the full system in a way that prepares it for the environment in which it will be operating.

SPDF

The latest guidelines lay out how a Secure Product Development Framework (SPDF) can help satisfy the FDA's requirements. Especially since "An SPDF is a set of processes that help identify and reduce the number and severity of vulnerabilities in products."

After all, each avoidable vulnerability, whether currently executable or not, brings a slightly greater risk to a healthcare organization or a person's home network. The FDA makes their views clear, stating "The greater the number of vulnerabilities that exist and /or are identified over time in a system which a device operates, the easier a threat can compromise the safety and effectiveness of the medical device."

However, understanding exactly how a device will be used and what the threat landscape will be in their unique environment, which likely varies from device to device, is a great challenge. To make sure this is being conducted correctly, the FDA wants manufacturers and their supplies to consider the devices intended use, potential for electrical interference, intended environments, and more.

The FDA's recommended considerations during early device development are:

- The device's intended use, indications for use, and reasonably foreseeable misuse;
- The presence and functionality of its electronic data interfaces;
- Its intended and actual environment of use;
- The risks presented by cybersecurity vulnerabilities;
- The exploitability of the vulnerabilities; and
- The risk of patient harm due to vulnerability exploitation.

Transparency

Transparency is nothing new to product security pros and it's been something Dr. Suzanne Schwartz, Director of Strategic Partnerships & Technology Innovation at the Center for Diseases and Radiological Health (CDRH) of the FDA, has been saying for some time.

When speaking with the Left to our Own Devices podcast, Dr. Suzanne Schwartz focused on the responsibilities held by the FDA. She said, "Our responsibility was to assure that the FDA and CDRH specifically were prepared to take on different types of hazards, whether they are physical or natural hazards or other types of events that may manifest as public health emergencies."

Driving this home, there were three overarching points that helped guide their decisions. They were Trustworthiness, Transparency, and Resilience.

The FDA is making transparency more and more a requirement via SBOMS and other methods that require the full disclosure of vulnerabilities, whether it be from OSS, Custom OSS, 3rd-party, off the shelf, or software developed in-house. Information on where to find SBOMs and supporting documentation must be directly on the label, meaning companies can't wait for an audit anymore– the full device SBOM must be ready to go from the moment it ships.

> In order to address these concerns, it is important for device users to have access to information pertaining to the device's cybersecurity controls, potential risks to the medical device system, and other relevant information. For example:
>
> - A failure to disclose all of the communication interfaces or third-party software could fail to convey potential sources of risks;
> - Insufficient information pertaining to whether a device has known but not disclosed cybersecurity vulnerabilities or risks may be relevant to determining whether a device's safety or effectiveness could be degraded; and/or
> - Labeling that does not include sufficient information to explain how to securely configure or update the device may limit the ability of end users to appropriately manage and protect the medical device system.
>
> *-FDA PMA 2023*

The FDA is going to be looking at your product security considerations. Beyond checking your device in a secure environment, stating "Manufacturers should take into account the larger system in which the device may be used." This approach is called the 'System of Systems' approach, not only testing and securing major components but even considering the 'dumb' devices whose output has a major impact on the greater system.

For this reason, sharing device-relevant information transparently benefits the entire ecosystem, from manufacturer to compliance officers, and ultimately the patients who will rely on these devices for their health. Repeating what we've seen in pillar three of the U.S. National Cybersecurity strategy, companies are expected to be held accountable, as well as their vendors, should an incident occur.

In addition, these companies must have a method for informing a patient of when a newly discovered vulnerability or incident impacts their device.

Cybersecurity strategy 2023 takeaways

Submission Documentation

As mentioned above, Trustworthiness, Transparency, and resilience has become a legislative requirement through the Omnibus.

Trustworthiness. This has been mentioned above indirectly through actions such as early vulnerability detection, elimination of vulnerabilities when possible, and implementation of an SPDF.

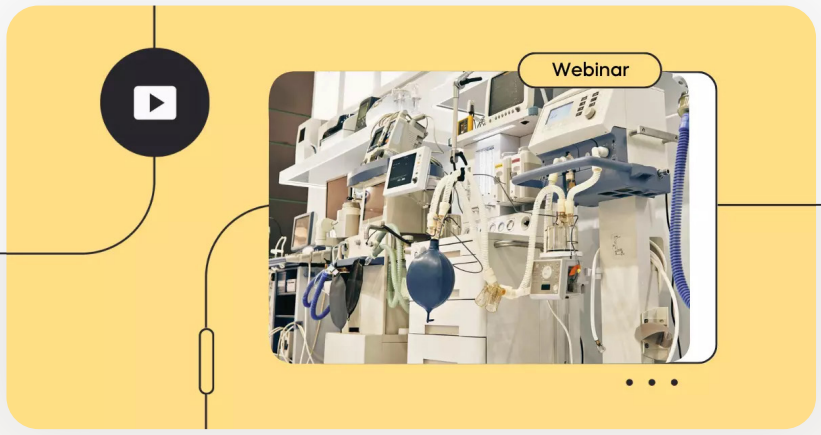
Transparency. Being able to convey what's inside a device demands that you have the latest information on-hand regarding components, software versions, and other information. This can be where that same SBOM that was generated during early development is continuously updated along with the patches and updates in the system.

Resilience. The ability to remain continuously compliant (point #4 in the omnibus bill) means that the device must be updateable via remote or physical connectivity. It also demands that companies continuously monitor their devices for newly discovered vulnerabilities and implement PSIRT in the event of a breach.

Ultimately, all product security measures taken to secure a device must not only work in a close environment amongst chosen devices. All activity needs to be backed up by documentation and scalable with a product security-first full lifecycle product security approach to make that happen in a scalable manner.

Adhering to the guideline's statement "Device cybersecurity design and documentation are expected to scale with the cybersecurity risk of that device," can be achieved with a centralized product security platform that replaces a mosaic of tools with one that delivers:

- Continuous SBOM management
- Automated vulnerability detection
- Continuous vulnerability management capabilities
- Triaging
- Red Team benchmarks
- Up to date data for active PSIRTs
- Workflows to automate the SBOM management, vulnerability discovery and management, VEX reports, and compliance docs



Making Medical Devices Cyber Compliant for the Omnibus

Managing security risk and eliminating vulnerabilities

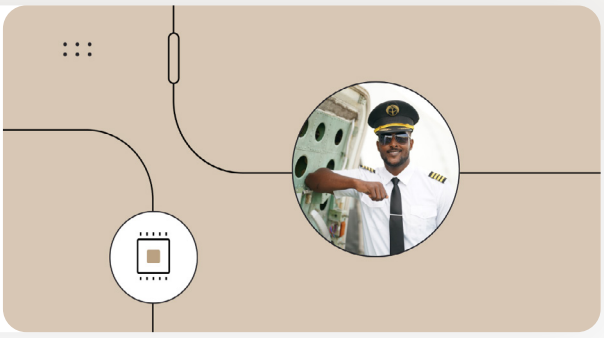
Managing the risk of devices doesn't mean rolling with the punches, it means thinking from the start about how to keep each individual device secure.

Ultimately, device safety, whether cybersecurity related or not, is a top priority. "Security risk management should be an integrated part of a manufacturer's entire quality system, addressed throughout the TPLC [total product life cycle]."

To achieve proper device security, product security professionals must have the ability to automatically triage and prioritize newly discovered vulnerabilities within their devices, which can be achieved with technologies such as the VM CoPilot. Vulnerability Management automations insure that as technologies advance, teams who rely on the same fixed number of resources can increase their impact without sacrificing security.

The VM Co-Pilot: An Automated Analyst for Product Vulnerability Management

August 7, 2023



Read about automating vulnerability identification and prioritization

Eliminating vulnerabilities

In the past, up until the announcement of RTA at the end of March 2023, the FDA requested that all vulnerabilities be mitigated. In the latest draft, the wording has been changed to add 'eliminate' instead of just 'mitigate'.

> ***A device should be designed to eliminate or mitigate known vulnerabilities. For marketed devices, if comprehensive design mitigations are not possible, compensating controls should be considered.***
>
> FDA PMA 2023

The FDA knows that no device can be 100% secure but taking steps to fully eliminate vulnerabilities has become a goal unto itself. This can be understood as the administration is open to mitigation methods, however when elimination is possible, it should be followed through.

Security risk management report

SBOMs act as a foundation for managing risk. “We're not asking for a software bill of material information just to ask for it. We are asking for it so we can use it. We do that by cross referencing SBOM information with other known information such as known vulnerabilities,” said Jessica Wilkenson. “So, what vulnerabilities need to be addressed? What vulnerabilities may be addressable later and how do I prioritize all of these things?”

When vulnerabilities are present in a device and they can’t be removed, they must be identified and reviewed throughout a device’s full lifetime, then run against CISA’s known vulnerability database.

A report should be generated explaining which vulnerabilities remain present in a device and the risk they bring with it.

In addition to containing the documentation elements listed above, the security risk management report should:

- Summarize the risk evaluation methods and processes,
- Detail the residual risk conclusion from the security risk assessment,
- Detail the risk mitigation activities undertaken as part of a manufacturer’s risk management processes, and
- Provide traceability between the threat model, cybersecurity risk assessment, SBOM, and testing documentation as discussed later in this guidance as well as other relevant cybersecurity risk management documentation.

-FDA PMA 2023

What's changed?

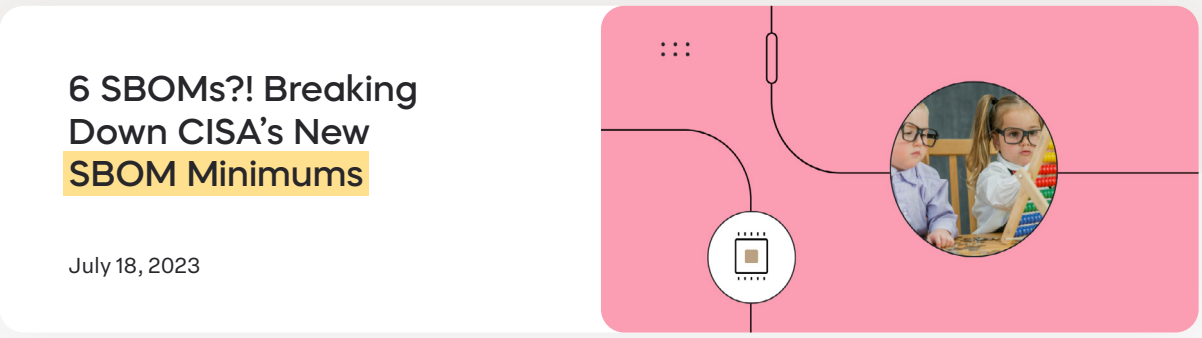
While much of the FDA's April 2022 PMA guidelines remain the same in September 2023, there are a few small changes that make a big difference.

Difference #1: Eliminate, not mitigate

The guidance now emphasizes that medical device manufacturers should design their products to "eliminate or mitigate known vulnerabilities." We believe that this subtle but significant change in wording means that companies must consider which components will be used and weigh the benefits vs. the vulnerability it brings. This shift from simply mitigating vulnerabilities is in line with CISA's approach to compiling a Type 1, or 'Design' Software Bill of Materials (SBOM). The goal is to identify and eradicate vulnerabilities at the source, reducing the risk posed by poorly secured components.

Why this matters

This new emphasis on elimination promotes a proactive approach to cybersecurity. It underscores the importance of assessing vulnerabilities at the component level from the earliest stages of development.



Learn the differences between SBOMs and how this impacts product security teams

Difference #2: Interoperability

Interoperability is a new section that requires companies to look at periphery cybersecurity challenges that may arise in the field– one of them the basic methods of communication between new devices and those already in the field.

The guidance recognizes the growing importance of interoperability in medical devices, highlighting potential cybersecurity considerations when devices interact with other medical devices, healthcare infrastructure, or general-purpose computing platforms. It highlights the need to assess security controls for common technology and communication protocols, ensuring the safety and effectiveness of the device.

> As part of a medical device system, a device may have cybersecurity considerations from interoperable functionality, including but not limited to interfaces with:
>
> - Other medical devices and accessories;
> - 'Other functions' as identified in the FDA's guidance "Multiple Function Device Products: Policy and Considerations;"
> - Interoperability with healthcare infrastructure (e.g., network, Electronic Medical Records, medical imaging systems); and
> - General purpose computing platforms.

It also adds, "When common technology and communication protocols are used to enable interoperability (e.g., Bluetooth, Bluetooth Low Energy, network protocols), device manufacturers should assess whether added security controls beneath such communication are needed to ensure the safety and effectiveness of the device (e.g., added security controls beneath Bluetooth Low Energy to protect against risks if vulnerabilities in the Bluetooth Low Energy protocol or supporting technology are discovered)."

Why this matters

This new addition acknowledges the potential introduction of new attack surfaces due to interoperability configurations between older and newer devices. To address this, the guidelines call for testing components for interoperability and adding security layers when necessary.

Difference #3: Source code access leniency

The 2023 guidance allows device manufacturers more flexibility regarding source code access.

While the previous 2022 version advocated custodial control of source code, the new guidance recognizes that manufacturers may face challenges related to licensing restrictions or supplier agreements. In addition, manufacturers are now encouraged to include plans for updating or replacing third-party software components.

> ***Manufacturers may not have control of source code due to licensing restrictions, terms of supplier agreements, or other challenges. While source code is not required to be provided in premarket submissions, manufacturers should include plans for how third-party software components could be updated or replaced if support ends or other software issues arise in premarket submissions.***
>
> FDA PMA 2023

Why this matters

There are three major points here. One is, the guidelines adapt to real-world challenges faced by manufacturers in managing source code. The next is that it reflects the FDA's commitment to holding vendors accountable, in line with the U.S. National Cybersecurity Strategy, and finally, it requires manufacturers to think not only until the end of their devices life, but a plan to manage components, should a relevant vendor stop issuing updates.

Difference #4: CISA Known Vulnerability Catalog

Manufacturers are now requested to identify all known vulnerabilities associated with their devices, including those listed in CISA's Known Exploited Vulnerabilities Catalog.

“As part of the premarket submission, manufacturers should also identify all known vulnerabilities associated with the device and the software components, including those identified in CISA’s Known Exploited Vulnerabilities Catalog.”

Why this matters

Instead of companies choosing which database to run their vulnerabilities against, the use of CISA’s catalog creates a national minimum database requirement. Beyond further aligning federal agencies, this move means that companies should be prepared to reveal all vulnerabilities that are related to the device, whether it is a risk to the product or not.

Difference #5: Further merging security and quality

The guidance emphasizes the connection between security and quality by stating that cybersecurity management plans can support security risk management processes described in the Quality System (QS) regulation. It even suggests the use of a Secure Product Development Framework (SPDF) to satisfy QS regulation with regards to cybersecurity.

The document states “A Secure Product Development Framework (SPDF) may be one way to satisfy the QS regulation”.

Why this matters

The latest guidelines take a further step in aligning product security with product quality. This was not only hinted at and mentioned throughout earlier drafts but it reflects a growing trend in various industries to unify safety and security considerations. It also changes the conversation from merely complying to going above and beyond the minimum requirements in the name of product quality.

What remains the same

Much of what we've seen in earlier drafts remains the same for the September 2023 PMA. Product security remains a critical part of quality while trustworthiness, transparency, and resiliency continue to lead in key decisions. Being able to demonstrate cyber-resilience through documentation from the beginning of development through market authorization and beyond must remain the top goal of medical device manufacturers.

As noble as it may be to agree with these high cybersecurity standards, someone has to actually manage and oversee all aspects. To reduce pressure on security teams, implement an SPDF, and scale product security activities, a dedicated product security solution is required.

The core elements of any approach to product security includes:

SBOM Management

The nature of SBOMs is that they need approval from multiple stakeholders to ensure that all teams are aligned with what is in the device. This goes beyond generation to managing an SBOM, meaning that with a centralized platform, such as the Product Security platform, teams can:

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 formats, 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

Once vulnerabilities are discovered, it takes time to understand their impact and prioritize accordingly. At scale, the task is nearly impossible. With the Product Security Platform, that has been changed with the Vulnerability Co-Pilot that automatically triages and prioritizes threats. This means teams can:

Understand the real risk impact - Cybellum analyzes your device software in incredible detail, then matches it with product vulnerability databases. Clearly understand which vulnerabilities post 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 - Gain contextualized insights based on Cybellum's medical-device 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.

Threat Modeling

> ***Threat modeling [is] a methodology for optimizing system, product, network, application, and connection security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.***
>
> FDA PMA 2023

Threat modeling allows teams to understand the risks to their devices and prepare mitigation methods to ensure security into the future. According to the guidelines, threat models should:

- **Evaluate and report potential concerns-** "Identify medical device system risks and mitigations as well as inform the pre- and post-mitigation risks considered as part of the cybersecurity risk assessment".
- **Consider and share the environment considered when testing-** "State any assumptions about the medical device system or environment of use (e.g., hospital networks are inherently hostile, therefore manufacturers are recommended to assume that an adversary controls the network with the ability to alter, drop, and replay packets);"
- **Source securely-** "Capture cybersecurity risks introduced through the supply chain, manufacturing, deployment, interoperation with other devices, maintenance/update activities, and decommission activities that might otherwise be overlooked in a traditional safety risk assessment process."

Compliance Management

Complying with the PMA guidelines requires a hard look at the full product security and compliance process. Cybellum's Product Security Platform allows teams to:

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 by automatically integrating these policies into your workflow.

Comply faster - 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.

As a bonus, 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)

Should a breach or incident occur, a company's Product Incident Response Team (PSIRT) are the first to respond. Made up of multi-disciplinary members with their own expertise, they demand the most up to date information to contain any damage. Using a centralized platform allows these response teams to:

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.

Manage it all in one place

From a managerial standpoint, it's critical that device security operations are continuously monitored. With the Product Security Platform's dashboards, 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.

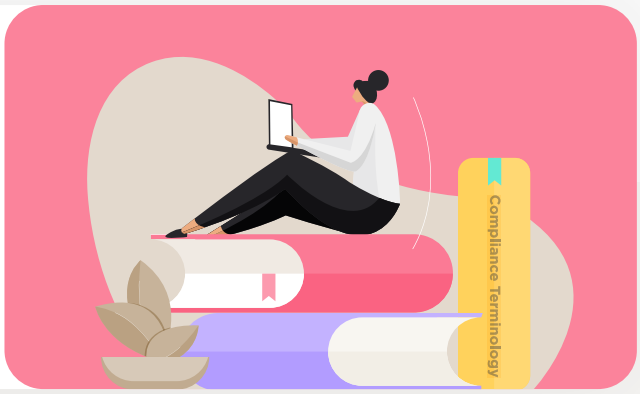
You can also see trends over time, tracking progress over time such as the percentage of products at risk, SLA tickets met, average resolution times, and more.

Dedicated product security solutions provide a comprehensive framework to comply with regulations, manage vulnerabilities, and ensure the security of medical devices throughout their lifecycle– all critical for both patient care and compliance.

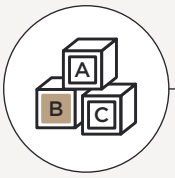
Remaining on the market and maintaining a secure upper-hand demands that product security be top of mind every step of the way.

Untangling Terminological Chaos

Product Security Glossary of Standards, Regulations, and More



Defining Key Terms



Building blocks of compliance

- **Standards**
  - **Definition:** Guidelines or best practices established by recognized organizations, professional bodies, or industry groups.
  - **Purpose:** Ensure quality, safety, reliability, and consistency of products, services, or processes across industries.
- **Compliance**
  - **Definition:** The act of adhering to or following established rules, regulations, policies, or standards.
  - **Purpose:** Conform to legal requirements, industry standards, internal policies, or ethical practices set by regulatory authorities, industry bodies, or organizations.
- **Regulatory Compliance**
  - **Definition:** Conformance to laws, rules, and regulations set forth by governmental or regulatory authorities.
  - **Purpose:** Adhere to requirements governing various aspects of a business, such as product security, safety, privacy, financials and environmental protection, to avoid fines, penalties, and legal action.

Differences

The ABCs of Compliance: Exploring Standards, Compliance, and Regulatory Landscape

- **Scope:** Standards focus on specific areas or industries, while compliance covers a broader range of rules, policies, or standards, including regulatory requirements. Regulatory compliance targets government-imposed regulations specifically.
- **Voluntary vs. Mandatory:** Standards can be voluntary or mandatory, based on context and industry. Compliance is generally expected, while regulatory compliance is mandatory due to governmental regulations.
- **Consequences:** Non-compliance with standards may harm reputation and competitiveness, while regulatory non-compliance can result in legal penalties, fines, and license suspensions or revocations.
- **Authority:** Standards are developed by professional organizations or industry bodies, while compliance and regulatory compliance are driven by adherence to governmental, industry, or organizational rules and regulations.

Standards

Navigating the Landscape of Standards

- **International Standards**
  - **Example:** ISO (International Organization for Standardization)
  - **Scope:** Global guidelines applicable across industries and countries
- **National Standards**
  - **Example**: ANSI (American National Standards Institute) in the United States
  - **Scope:** Country-specific guidelines developed by national standard-setting organizations
- **Industry-specific Standards**
  - **Example:** HIPAA (Health Insurance Portability and Accountability Act) for healthcare
  - **Scope:** Standards tailored to the unique requirements and practices of specific industries
- **Company-specific Standards**
  - **Example:** Apple's Supplier Code of Conduct for its supply chain partners
  - **Scope:** Internal guidelines and best practices developed by individual organizations to meet their specific needs and goals

Benefits of Standards

Reaping the Rewards of Adherence to Standards

- **Improved Product Quality, Security, Safety, and Reliability**
  - Consistent performance and better customer experience
  - Reduction of compromises, accidents, defects, or failures
- **Increased Consumer Trust and Market Competitiveness**
  - Enhanced brand reputation and credibility
  - Competitive advantage through adherence to best practices
- **Facilitated International Trade and Collaboration**
  - Common language for organizations and industries across countries
  - Simplified compliance with global regulatory requirements
- **Risk Mitigation and Avoidance of Fines**
  - Reduced exposure to legal penalties and financial loss
  - Proactive management of potential risks and liabilities

Compliance Management

The Four Pillars of Effective Compliance Management

- **Risk Assessment**
  - Identification and evaluation of potential compliance risk
  - Prioritization of risks based on their impact and likelihood
- **Compliance Monitoring**
  - Regular audits and reviews to ensure adherence to rules, policies, or standards
  - Tracking of regulatory changes and updates
- **Training and Education**
  - Development and implementation of employee training programs
  - Building awareness of compliance requirements and best practices
- **Reporting and Documentation**
  - Collection and analysis of compliance-related data
  - Record-keeping and reporting to demonstrate compliance efforts

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Top medical device manufacturers such as Danaher and Siemens use Cybellum's Product Security Platform and services to manage cybersecurity risk and FDA compliance across business units and lifecycle stages. From SBOM to Vulnerability Management, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

To learn more visit cybellum.com

Learn more about Product Security

Blogs

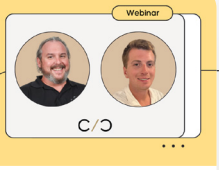
Introduction to Medical Device Security Standards and Regulations

Rolling Regulations: Embrace Them, Don't Chase Them

Keeping the Software Supply Chain Accountable with SBOMs

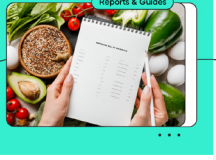
Podcasts

Knowledge Base



Countdown ep.1: No time to Comply)FDA Omnibus)

Learn More →



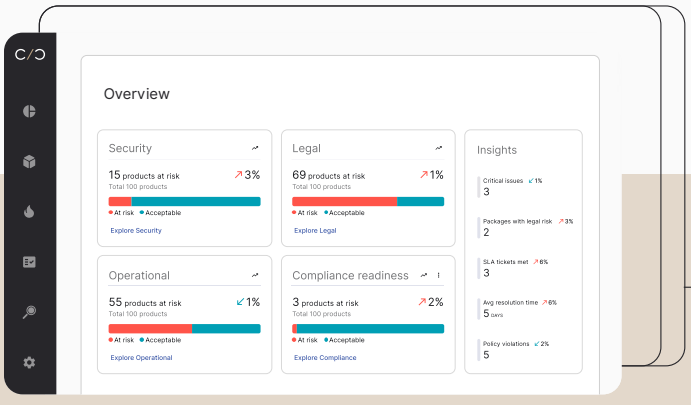
SBOM for Connected Devices: Getting it Right

Learn More →

How Medical Device Makers Can VEX Cyber Threats and Secure the Healthcare Supply Chain

Learn More →

More about the Product Security Platform



Follow us for news and updates cybellum.com