Published by the U.S. National Committee of the IEC, a committee of the American National Standards Institute Vol. 19, No. 1 - Winter 2024

FOOD AND DRUG OMNIBUS REFORM ACT OF 2022 (FDORA) AND MEDICAL DEVICE CYBERSECURITY

Ken Zalevsky – CEO at Vigilant Ops

On December 29, 2022, the president of the United States signed into law the Food and Drug Omnibus Reform Act of 2022 (FDORA) as part of the Consolidated Appropriations Act, 2023. This law introduces various provisions aimed at improving medical device cybersecurity, which will have considerable effects on medical device manufacturers and their consumers. Through FDORA, the United States Food and Drug Administration (FDA) was granted the legislative authority to require cybersecurity documentation from medical device manufacturers.

In the medical device industry, this recently-executed legislation represents a dramatic shift in the regulatory landscape. While FDA has authored numerous guidance documents, with various recommendations for medical device manufacturers, this legislative authority is a whole new ball game.

WHAT THIS MEANS TO MEDICAL DEVICE MANUFACTURERS

We'll start by taking a look at the scope of the legislation and the description of the medical devices covered. According to the document, the legislation applies to all **cyber devices**, which are defined as any device that has the **ability to connect to the internet** and **contains technological characteristics that could be vulnerable to cybersecurity threats.** In other words, this legislation is applicable to most medical devices. While there are undoubtedly devices that are standalone with no ability to communicate and others that have no technological characteristics (a tongue depressor comes to mind), for most medical device manufacturers, this law applies to some device or multiple devices in their portfolio. And, to add urgency to the matter, this law is actually enforceable at this very moment.

NON-COMPLIANCE RESULTS IN PENALTIES SOONER RATHER THAN LATER

According to the legislation, these cybersecurity requirements went into effect 90 days after the date of the Act, on March 29, 2023. While manufacturers were given until October 31, 2023, to begin submitting the appropriate documentation, compliance with these legislative requirements is now expected.

The legislation spells out the consequences of non-compliance by adding this phrase to the Federal Food, Drug, and Cosmetic Act (FD&C): "The failure to comply with any requirement under section 524B(b)(2) relating to ensuring device cybersecurity" to the Prohibited Acts and Penalties of the FD&C. This chapter of the FD&C covers, in great detail, those activities which will incur penalties and begins with, "The folllowing acts and the causing thereof are hereby prohibited." In other words, failure to comply with cybersecurity requirements is prohibited by law and is now considered alongside prohibited acts such as mislabeling and misbranding.

VULNERABILITY PLAN

For medical device manufacturers, the cybersecurity requirements begin at the top of page 3538 in section (b), describing how manufacturers should handle vulnerabilities. The requirement is to "submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket vulnerabilities and exploits..."

While it may seem contradictory to require a postmarket plan in a premarket submission, the message conveyed to manufacturers is that cybersecurity cannot be an afterthought. The cybersecurity of the device should be considered as far upstream in the development lifecycle as possible. Requirement (2) under section (b) contains various references to the development lifecycle of devices, beginning with the recommendation for secure processes from development all the way through to the availability of postmarket updates and patches to address cybersecurity vulnerabilities. In addition, the ability to respond to vulnerabilities in "a reasonable time" implies frequent, if not continuous, vulnerability monitoring. This is another key consideration for medical device manufacturers as they build or adapt processes to support compliance.

SOFTWARE BILL OF MATERIALS

Requirement (3) under section (b) requires manufacturers to provide a software bill of materials, "including commercial, open-source, and off-the-shelf software components." As a list of software components in a device, the SBOM makes sense and is easy to understand. As always, however, the danger lies in the details. Knowing what an SBOM is and consistently, reliably generating and maintaining an SBOM for each device are two different stories. Then there is the sharing dilemma.

Some device manufacturers are debating the question of sharing SBOMs, due to some very real concerns about exposing vulnerable components to bad actors. While sharing SBOMs with FDA is a must-have, some are still looking at sharing with consumers as a nice-to-have. This view will need to adapt to the seemingly eventual demand for SBOMs from consumers.

Fortunately, there are many SBOM resources available to help manufacturers, from minimum SBOM requirement documentation to open-source and commercial tools available to assist in automating the SBOM process, depending on where the manufacturer is in their SBOM journey. Given the breadth of the SBOM topic and the lack of homogeneous adoption, we won't attempt to cover the topic here; however, we have included a Resources section at the end of this article with SBOM and other references.

SUMMARY

In this article, we highlighted FDORA content with specific impact on medical devices and the resulting requirements for medical device manufacturers. While medical device cybersecurity continues to evolve, manufacturers need to evolve, as well. By prioritizing cybersecurity and the development of supporting processes and procedures, they will be well on their way toward compliance, now and in the future.

RESOURCES

This article detailed the cybersecurity requirements found in the Consolidated Appropriations Act, H.R. 2617, which is available at https://www.congress.gov/117/bills/hr2617/BILLS-117hr2617enr.pdf

For additional details from FDA on the application of the reviewed legislation to medical devices, please refer to the following guidance documents from FDA:

» FDA Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

» FDA Postmarket Management of Cybersecurity in Medical Devices https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

For help with the software bill of materials (SBOM), please refer to the following:

» The Cybersecurity & Infrastructure Security Agency (CISA) Software Bill of Materials https://www.cisa.gov/sbom

» International Medical Device Regulators Forum (IMDRF) – "Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity" https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity

» Achieve SBOM Compliance with the InSight Platform from Vigilant Ops https://www.vigilant-ops.com/