MEDTECH INSIGHT
CITELINE COMMERCIAL

12 Apr 2022 | **Analysis**

FDA's Schwartz Says New Draft Cybersecurity Guidance Addresses Emerging Threats

Agency shifts focus to software, removes tiered risk assessments

by Brian Bossetta

Suzanne Schwartz, director of the US FDA's Office of Strategic Partnerships and Technology Innovation, tells *Medtech Insight* that recent cyberattacks have crippled hospitals networks, putting many patients at risk.

The US Food and Drug Administration's *latest draft guidance* on medical device cybersecurity has evolved since the agency's last update in 2018 because so has the threat, says Suzanne Schwartz, director of the Office of Strategic Partnerships and Technology Innovation within the agency's device center.

Schwartz told *Medtech Insight* on 11 April that the new guidance the agency issued on 8 April that essentially replaces its 2018 version (which itself updated the agency's original 2014 draft) outlines a comprehensive approach device manufacturers can take to address cybersecurity concerns throughout the total product life cycle of their products – "from the earliest stage of development all the way out."

The newest set of recommendations from the agency also asks industry to consider cybersecurity as integral to the FDA's Quality System Regulation (QSR), which requires a manufacturer to establish and maintain procedures for validating a device's design.

The draft guidance further recommends that device firms establish a Secure Product Development Framework (SPDF) to reduce the number and severity of product vulnerabilities to better hit QSR benchmarks.

As the FDA makes clear in its document, cyberattacks against hospital systems and networks can directly result in harm to patients. (Also see "*FDA Issues Long-Awaited Guidance On Device Security For Premarket Submissions, Seeks Industry Feedback*" - Medtech Insight, 8 Apr, 2022.)

Dennis Gucciardo, a partner at the law firm Morgan Lewis who counsels device manufacturers, told *Medtech Insight* cyberattacks pose major risks and cited the attack in April 2021 across 42 sites in the US that delayed high-tech radiation treatment for many cancer patients.

Gucciardo also said in an 8 April interview that a ransomware attack on a hospital's network could take infusion pumps offline or could alter diagnostic data resulting in delayed or inaccurate treatments.

Pointing to an obvious difference in the most recent draft – 50 pages compared to just 9 in the agency's 2014 draft – Schwartz said the FDA's much-anticipated document provides device makers the tools needed to not only improve the efficacy of their products, but better shield them from hackers.

> ***"Right now it's really key to have manufacturers understand the aspect of free markets that extends well beyond the device becoming authorized to go on the market." – Suzanne Schwartz***

As Schwartz noted, the bulk of the 2022 draft compared to earlier versions reflects its detail and the input the agency received from industry and other stakeholders from the first iterations of the guidance and the "advancement of what we have learned and what we expect to see with respect to manufacturers securing their devices from the time they were designed and developed."

Reorganizing the guidance with the life cycle of the device in mind produced a draft that is a "significant improvement" over the agency's prior proposed guidances, Schwartz said.

Schwartz also pointed to the document's title, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," and its references to the QSR. "This is important in further underscoring the expectation that the FDA has for security being managed throughout the lifetime of that device, not just merely at the time of the device being deployed into the marketplace," Schwartz said, "but that there are expectations of maintaining the quality systems throughout the device's life cycle."

While the FDA has proposed to replace its current QSR with a next-generation quality systems rule – the Quality Management System Regulation – Schwartz said it was too soon to say if there would need to be an update to the guidance when the QMSR ultimately goes into effect. (Also see "*10 Things You Need To Know About FDA's Proposed Quality Management System Regulation*" - Medtech Insight, 23 Feb, 2022.)

"If you are asking about some additional, future changes, I think that's out of scope at present. We'd have to come back to that at some other point," she said. "Right now it's really key to have manufacturers understand the aspect of free markets that extends well beyond the device becoming authorized to go on the market. It's really about their thinking well in advance of how they are going to make sure their device is able to be managed from a cybersecurity perspective throughout the device's lifetime."

Citing the importance the FDA puts on industry concerns, Schwartz said the agency removed the two-tiered risk management approach to device security suggested in the 2018 guidance because manufacturers viewed the stratification levels – Tier 1 for devices considered "higher risk" and Tier 2 for "standard risk" – as confusing. The consensus among industry, Schwartz said, was that adding yet another hierarchy to the already established risk classifications of devices was too difficult to sort through.

QMSR Quick Take: Attorney Dennis Gucciardo

By Shawn M. Schmitt

01 Mar 2022

Morgan Lewis partner Dennis Gucciardo gives a quick take on the US FDA's proposed Quality Management System Regulation. The QMSR would replace the agency's current Quality System Regulation.

Read the full article here

"So instead in this guidance we speak about the important documentation and testing that needs to be done by a manufacturer and what we would want to see in that premarket submission commensurate with the risk of that device from a security perspective," she explained.

Another major distinction between the 2022 and 2018 drafts concerns the agency's focus on software rather than hardware.

> ***"The FDA is saying, though you didn't design that platform and can't control it, you still need to consider the vulnerability of it in***

your risk management." – Dennis Gucciardo

Whereas the 2018 guidance referred to the cybersecurity bill of materials, or CBOM, the 2022 guidance features the software bill of materials, or SBOM, which asks manufacturers to provide details on a device's software, rather than the hardware of CBOM, which industry saw as too burdensome on top of other regulatory considerations.

As with the tiered system, Schwartz said the agency changed its thinking after learning that addressing software first would go further in providing the agency with a better tool for risk mitigation and assessment.

"It's going to be a hard enough challenge just in terms of bringing the ecosystem to operationalize a software bill of materials, then execute and implement that," she said. "So let's get that done first. Let's make sure we have a feasible and actionable SBOM before we move on to something which is far more aspirational than software."

Gucciardo explained that the SBOM outlined in the 2022 guidance asks a manufacturer to consider a "piece of the puzzle" that a manufacturer did not create.

For example, a device may require another company's platform or server in order to operate, such as Windows, but should that third-party system be compromised, then so would that device.

"The FDA is saying, though you didn't design that platform and can't control it, you still need to consider the vulnerability of it in your risk management," Gucciardo said. "You have to take some responsibility for that piece."

"The third-party software is a critical aspect, absolutely," Schwartz said, adding that without it a health care provider organization or other user would be unable to address risk and put in place the necessary safeguards in advance. "That information becomes very, very important, and ultimately device manufacturers are responsible for providing that information to us as they are for any component parts."