Stratigos Security has analyzed the newly released FDA premarket guidance for medical device cybersecurity (as of July 2025). This is an evolution of their earlier guidance (published September 2023), with a few significant additions and very minor modifications to existing guidance details. In general, these changes align with what has been discussed publicly in presentations, media quotes, webinars, and interim clarifications, as well as the post-market guidance, published in December 2016. The vast majority of these changes appear in Section VII (pp. 30-36), which is totally new in the update.

From discussions, we understand that the FDA has updated this guidance based on lessons learned from the prior several years of reviewing applications, addressing post-market surveillance gaps, and conversations with the broader healthcare community (including us, MedCrypt, medical device makers, and cybersecurity researchers). Below are a few details of what has changed, as well as the significance.

- **Clarification** (section VII B) that a "cyber device" includes any device with software and a digital hardware or radio frequency interface (including USB, NFC, Ethernet, Bluetooth), even if disabled by default or hidden behind an external enclosure. This was previously stated in an interim clarification document, published in April 2024.
- **Clarification** (section VII C 1) that a Cybersecurity Management Plan be provided for all regulatory submissions, regardless of whether they were previously required.
- **Clarification** (section VII C 2) that manufacturers include related systems when taking steps to provide reasonable assurance of cybersecurity, which may include those they manage, as well as those from other vendors and healthcare providers (among others). This is consistent with public statements made and with the intent of the original guidance.
- **Clarification** (section VII C 3) that SBOMs be provided as a part of pre-market processes. This is consistent with public statements, was specified in the PATCH Act (signed into law December 2022), and was previously stated in an interim clarification document, published in April 2023.
- **Clarification** (section VII D) for manufacturers of what constitutes changes to devices that may affect cybersecurity versus those that are unlikely to. This is consistent with public statements and feedback to manufacturers made since publication of the prior pre-market guidance.
- **Clarification** (section VII D 2) that submissions describe vulnerabilities discovered since the last submission that could affect safety and effectiveness (aka "uncontrolled risks"), as well as how they were remediated. This is consistent with the existing postmarket guidance.
- **Additional requirement** (section VII D 2) that a Cybersecurity Management Plan account for reports from third-parties (such as cybersecurity researchers), with provisions to receive, assess, coordinate disclosure, and address vulnerabilities and exploits. This aligns with the existing post-market guidance, which requires that manufacturers have this capability, though it is the first time documentation has been required during a pre-market submission.
- **Clarification** (section VII D 2) that cybersecurity capabilities must be updated to match current risks - including those from evolving threats, new technologies (such as addition of network or radio frequency capability), and new environments (such as in a hospital versus a lab) - not just those assessed when the device was first approved. This is consistent with the intent of the prior pre-market guidance, as well as public statements since.
- **Minor updates** to add new standards that have been developed (such as ANSI/AAMI SW96) and to reference other FDA documentation published since the prior final guidance document (such as 89 FR 7496).