Health-ISAC®
Collaborating for Resilience in Health

ANNOUNCEMENTS

Health-ISAC Fall America Summit FDA Town Hall Recap

●●● TLP:WHITE Dec 10, 2025

On December 2nd, the Health-ISAC Fall Americas Summit convened healthcare leaders and regulators to address the evolving medical device cybersecurity landscape. The FDA's Division Director for Medical Device Cybersecurity and a Policy Analyst provided direct insights into current regulatory priorities. The briefing included revisions to the premarket guidance with an emphasis on the alignment with CFR20, clarified the definition of a cyber device and submission expectations aligned with section 524B obligations. The FDA also shared common submission deficiencies include inadequate threat modeling, incomplete risk assessments, missing or outdated SBOMs, weak penetration testing, and insufficient security architecture detail The Summit reinforced the FDA's expectation that manufacturers elevate cybersecurity programs to meet regulatory standards. Healthcare Technology Management leaders are urged to operationalize guidance now; embedding SBOM tracking, enforcing patch timelines, and aligning procurement with secure design principles to transform compliance into resilience and safeguard patient safety.

On December 2nd, the Health-ISAC Fall Americas Summit provided members with a unique opportunity to engage directly with regulators on the evolving medical device cybersecurity landscape. Featured FDA speakers included the Division Director for Medical Device

Cybersecurity and a Policy Analyst for Cybersecurity, with participation available both in person and virtually to maximize accessibility. Regulators shared current perspectives, including updates to premarket cybersecurity guidance and insights into common submission challenges, underscoring the Summit's role as a key forum for advancing dialogue between industry and the FDA.

Recent updates emphasize compliance with CFR 20 requirements and expanded the use of the E-Star platform as a requirement for 510(k) and De Novo submissions. The FDA clarified the definition of "cyber devices," which includes any device connecting to the internet, intentionally or unintentionally, as well as USB ports and wireless or hardwired networks. Section 524B requires manufacturers to consider related systems holistically, ensuring secure connections, device safety, and control elements. Health-ISAC recommends that procurement contracts include clauses addressing secure architecture, patch management processes, and vulnerability disclosure practices.

Section 524B also introduces critical obligations: manufacturers must provide cybersecurity management plans, patch timelines, and vulnerability tables, while maintaining machine-readable SBOMs. These requirements strengthen transparency and resilience, enabling proactive monitoring of end-of-life and end-of-support components.

The FDA noted recurring submission issues, including inadequate threat modeling, incomplete risk assessments, missing or outdated SBOMs, insufficient security architecture detail, and weak penetration testing practices. Taken collectively, these issues suggest a tracer methodology in submission documentation to connect the vulnerabilities associated with components in the SBOM to threat assessments, security risk analysis, mitigation techniques, and the testing to demonstrate adequate control effectiveness.   These deficiencies highlight a need for manufacturers to elevate their cybersecurity programs to meet regulatory expectations.

In Q&A, the FDA clarified that “state-of-the-art” refers to secure, research-backed best practices rather than cutting edge technologies. SBOMs must clearly document unsupported components, and vulnerability matching requires good-faith effort despite CVE complexity. Post-quantum cryptography remains a priority, with FDA active in HSCC working groups. Despite workforce challenges, cybersecurity reviews remain a top priority.

Alert ID 3d21c3e6

View Alert

Share Feedback

was this helpful? 👍 | 👎

Tags Medical Devices, FDA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Download Health-ISAC’s Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**