
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
cybersecuritysummit.org
RESILIENCE UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

What You Need to Know

to Start Implementing the FDA's New Medical Device Security Requirements

NETSPI

Ron Kuriscak

Managing Director

NETSPI

Steve Currie

Senior Director of Cybersecurity Operations

Abbott

Setting the Stage — A Brief History

- On December 29, 2022, the Consolidated Appropriations Act, 2023 ("Omnibus") was signed into law:
  - Section 3305 - Ensuring Cybersecurity of Medical Devices

The Omnibus Bill gives statutory authority to the FDA in regulating cybersecurity in medical devices

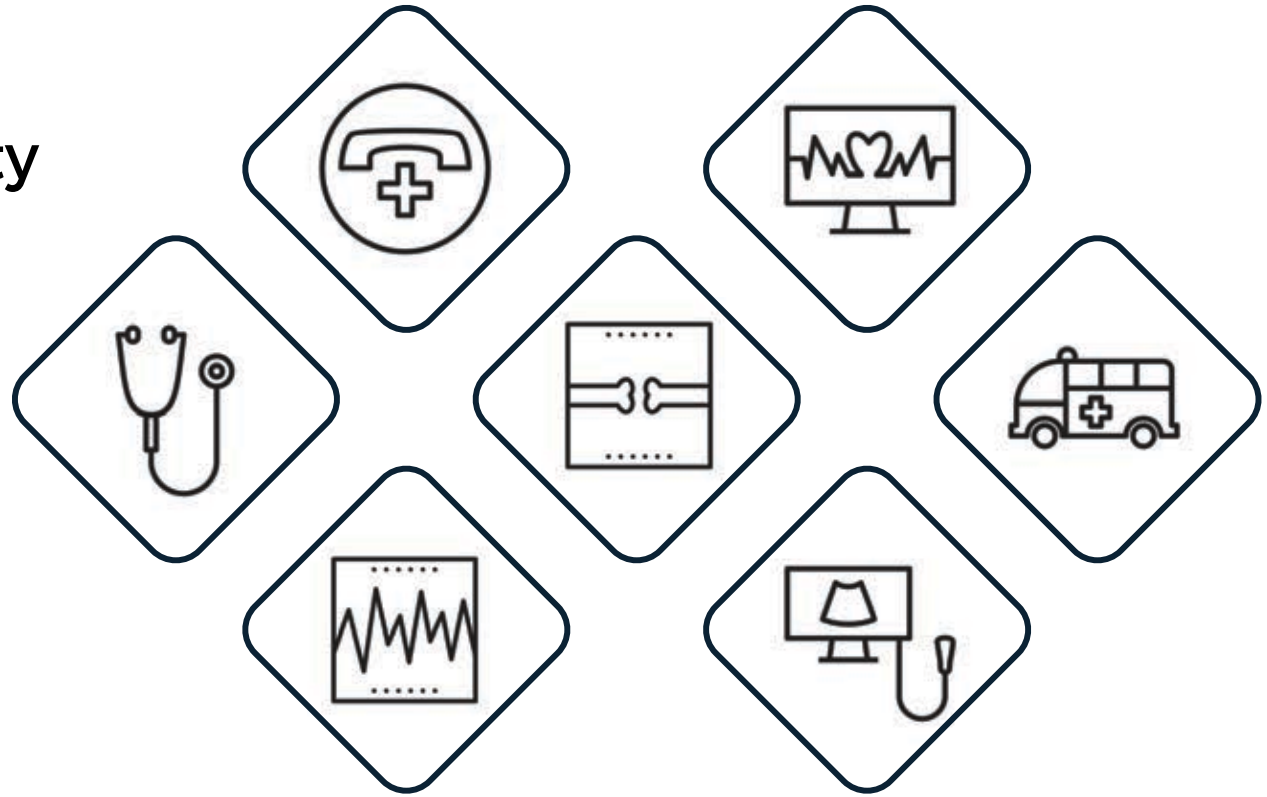
- Enforcement Capabilities

All devices that contain software, are able to connect to the internet, or may be vulnerable to cybersecurity threats must comply with these requirements

NETSPI

Nuances of Medical Device Security

- Development (SDLC)
- Device Control / Connectivity
- Shadow IT
- Connected Devices
- Data Protection
- Encryption / Device Communication
- Patient safety…



NETSPI

The Omnibus Rule

1. FDA now has dedicated funding for enforcement ($5M)
2. The Omnibus finalized guidance on:
    - Reasonably updated patch / update cycles
    - Medical devices are moving toward secure by design & secure lifecycle concepts
3. The latest update gives a definition of a “cyber device”
    - Includes software validated, installed, or authorized by the sponsor, indicating its integral role in device functionality.
    - Must possess the ability to connect to the internet.
    - Encompasses any technological characteristics that have been validated, installed, or authorized by the sponsor, which could potentially be susceptible to cybersecurity threats.

NETSPI

The Omnibus Rule (Cont'd)

- "…a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures."
- "…design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device."
- "…provide a software bill of materials, including commercial, open-source, and off-the-shelf software components."
- "…comply with such other requirements through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure."

Requirements of Submitting Plan to FDA

- Develop a strategy for monitoring, identifying, and addressing cybersecurity vulnerabilities and potential exploits
- Plan for addressing vulnerability disclosures and establishing incident response protocols
- Plan for routine post-market updates and patches

NETSPI

Breach Notification Guidelines and Incident Reporting

- Report certain cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours after a substantial incident
- Report ransomware payments within 24 hours

Note!

These requirements won't go into effect until late 2024 or 2025 when the final rulemaking is expected.

NETSPI

Key Takeaways

1. FDA now has dedicated funding
2. The Omnibus finalized guidance on:
    - Reasonable patch update cycles
    - Secure by design
3. Updated definition of a “cyber device”
    - Includes software validated, installed, or authorized by the sponsor, indicating its integral role in device functionality.
    - Must possess the ability to connect to the internet.
    - Encompasses any technological characteristics that have been validated, installed, or authorized by the sponsor, which could potentially be susceptible to cybersecurity threats.

NETSPI

Visit Us in the Expo Hall!

Stop by NetSPI's table for swag and to learn why we're the global leader in offensive security.

NETSPI