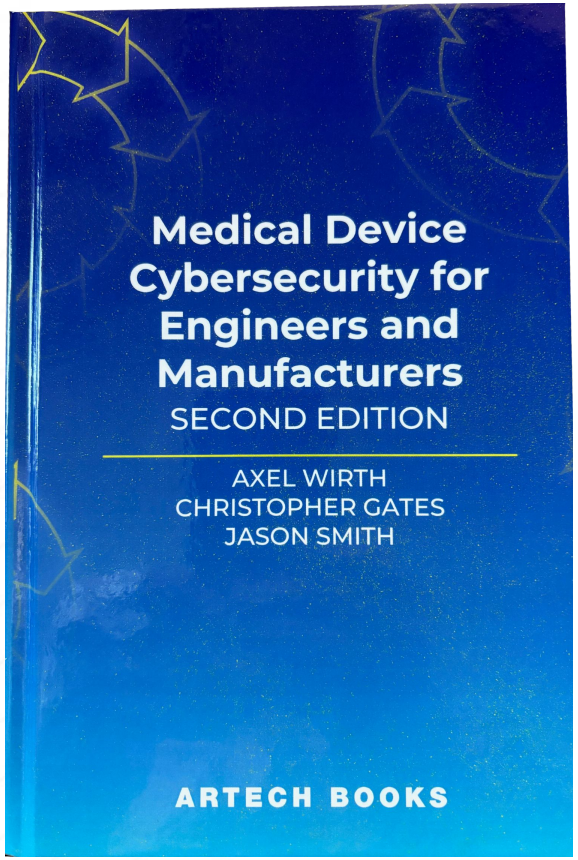
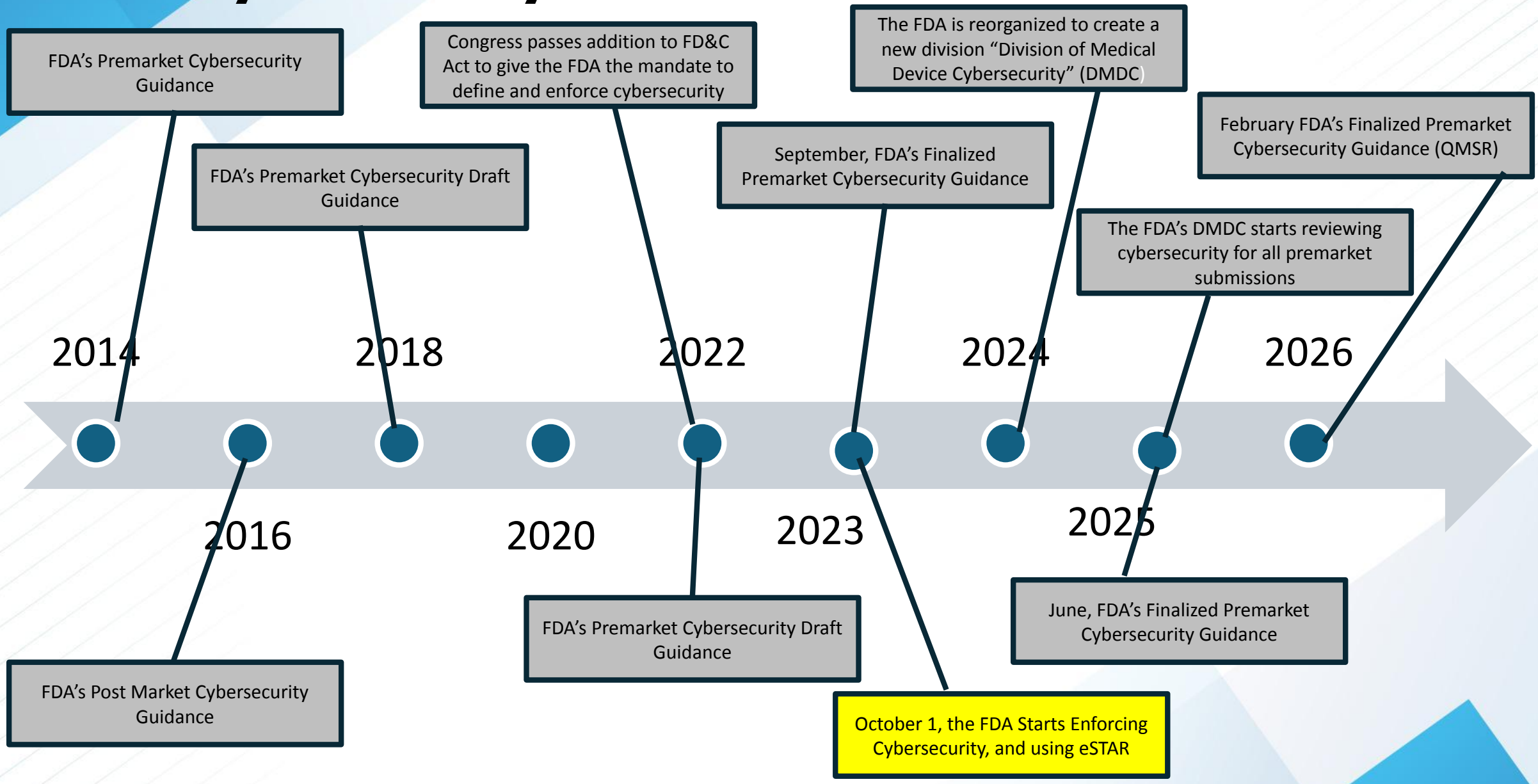
arsMedSecurity

arsMedSecurity Founder and CEO



FDA's Cybersecurity is Not New… Just More Extensive.



Size Doesn’t Matter

The Safety Risk Doesn't Matter

The Lack of Communications Doesn’t Matter

Waiting Until Late into Development

Your Developers Have Not Been Trained In Cybersecurity

Be Careful Choosing Your Partners

https://hms.harvard.edu/news/deaths-rose-emergency-rooms-after-hospitals-were-acquired-private-equity-firms

The FDA is Very Detailed In What It Wants

1) Security Risk Management Plan
2) Threat Model Report
3) Cybersecurity Risk Assessment Report
4) Software Bill of Materials
5) SBOM Support Report
6) Software Component Safety and Security Assessment Report
7) Vulnerabilities with Uncontrolled Risk Report
8) Unresolved Anomalies Risk Management Report
9) Cybersecurity Metrics Report
10) Cybersecurity Controls Report
11) Architecture Views Report
12) Cybersecurity Testing Report
    - Fuzz Testing (APIs and digital communication interfaces)
    - SAST Testing
    - Malformed User Inputs Testing
    - Mitigation Effectiveness Testing
    - SCA
    - Penetration Testing
    - SBOM Monitoring
13) Cybersecurity Labeling Report
14) Risk Management Report

$9.8 Million settlement for False Claims on Cybersecurity

DOJ Secures First of Its Kind Cybersecurity False Claims Act Settlement

On July 30, 2025, the U.S. Department of Justice ("DOJ") announced that biotechnology company Illumina Inc. agreed to pay $9.8 million plus interest to resolve allegations that it misrepresented compliance with federal cybersecurity requirements for medical device software. The settlement resolves a whistleblower suit brought under the False Claims Act ("FCA") by a former Illumina employee, in which the government later intervened.

The complaint alleged that, from January 2016 to April 2023, Illumina failed to incorporate adequate cybersecurity into the design, development, installation, and marketing of certain products used for research and clinical purposes. According to the relator, Illumina also failed to maintain adequate product security programs, correct known cybersecurity vulnerabilities that created vulnerabilities, or provide sufficient support for personnel and systems tasked with product security. During this period, the company allegedly certified to the U.S. Food and Drug Administration ("FDA") that its products complied with applicable cybersecurity requirements despite these deficiencies.

Hospitals Want Cybersecurity Too

A study* of 605 healthcare executives in the US, UK, and Germany involved with medical device purchasing:

- 75% of organizations increased their medical device and operational technology security budgets over the past 12 months
- 79% are willing to pay a premium for devices with advanced runtime protection or built-in exploit prevention
- 35% now identify operational technology systems like medical devices as their biggest cybersecurity concern
- 75% say that cyber incidents have caused at least a moderate patient care impact
- 32% say security incidents have not only affected their trust in specific vendors, but they also now require additional security verification from previously trusted vendors.
- 83% of healthcare organizations now integrate cybersecurity standards directly into their RFPs
- **46%** have declined medical device purchases due to cybersecurity concerns

*RUNSAFE SECURITY'S 2025 MEDICAL DEVICE CYBERSECURITY INDEX

The “R” Word…

- **Safety Risk Management**
  - Well-known and utilized in medical device development for the last 50 years
  - Process to analyze and assess harm to patients and the environment.
  - Based on likelihood/P1/P2
  - Based on the premise of naturally occurring events
  - Time frames of months and years
  - Informs the decision to implement mitigating controls vetted by security

- **Security Risk Management**
  - New emergent process
  - Different people and different tools
  - Based on Severity and Exploitability, no “likelihood.”
  - Process to analyze and assess negative impacts to the manufacturer, including:
    - Harm to patients and the environment (feeds into Safety Risk Management)
    - Loss of intellectual property
    - Financial impact of fines
    - Loss of consumer confidence
    - Stock prices
    - Loss of business
  - Assumes malicious intent and hostile environments
  - Time frames of days and weeks
  - Informs the decision to implement security mitigations vetted by safety

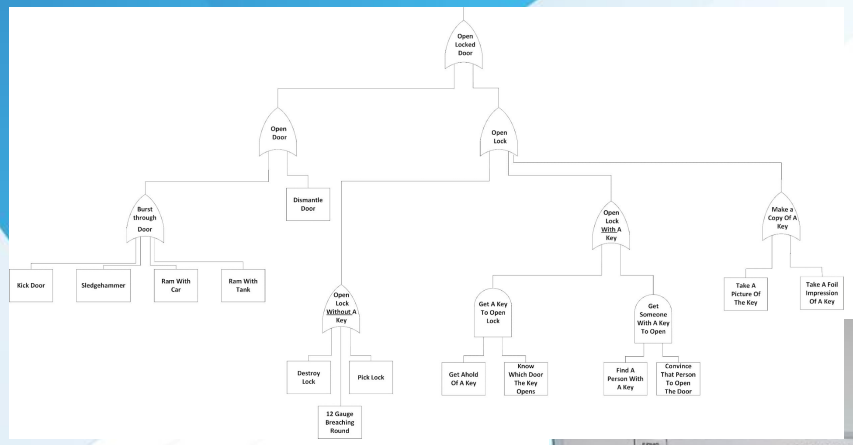
As defined by ISO 14971; The FDA; AAMI TIR57

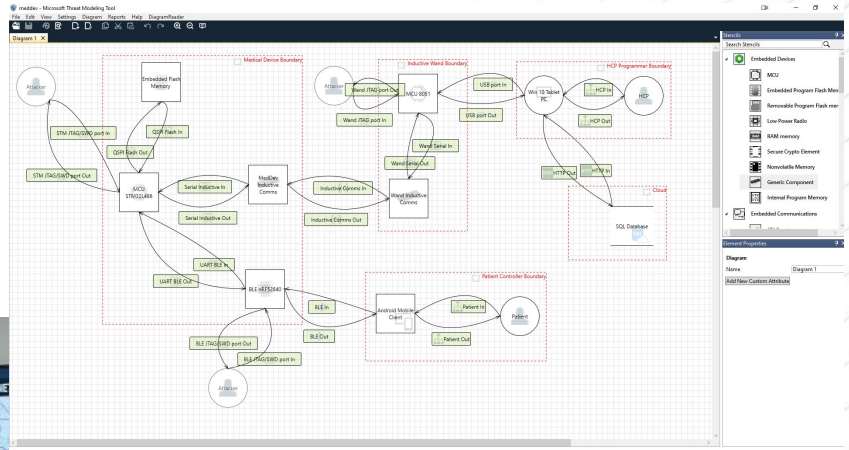
Software Product Development Framework (SPDF)

Standard security processes to be included in the development lifecycle

- **IEC 81001-5-1: 2021 Health software and health IT systems safety, effectiveness, and security – Activities in the product life cycle**
  - A medical device-specific standard for 62443-4-1 compliance.
  - Harmonized to the EU's MDR
  - A recognized standard by the FDA

Threat Modeling





- STRIDE Per Element
  - Global System
- Process Threat Modeling
  - Supply chain
  - Manufacturing
  - Deployment
  - Interoperation
  - Updates
  - Decommissioning

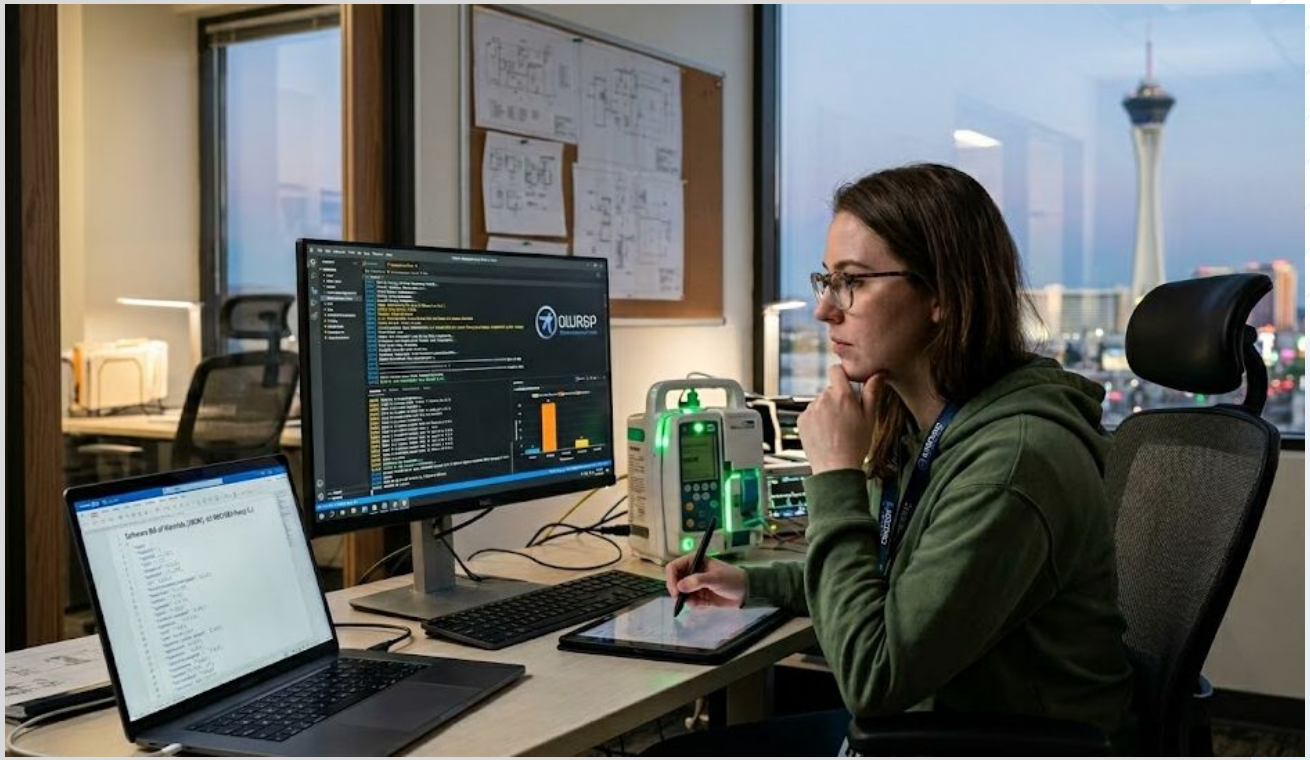
SBOM: Software Ingredients List

- An “SBOM” or “software bill of materials” is a list of ingredients in your software project.

- Specifically, an SBOM is a formal, machine-readable inventory of Third Party Software Components (“TPSC”) and dependencies, information about those components, and their hierarchical relationships.

- An Excel spreadsheet is not an SBOM! An SBOM is a JSON file formatted to CycloneDX or SPDX
- Including such software components as:
  - Libraries
  - Frameworks
  - operating systems
  - communication stacks

- Each component needs:
  - Supplier name
  - Component Name
  - Version
  - Unique Identifier
  - Dependency
  - Hash

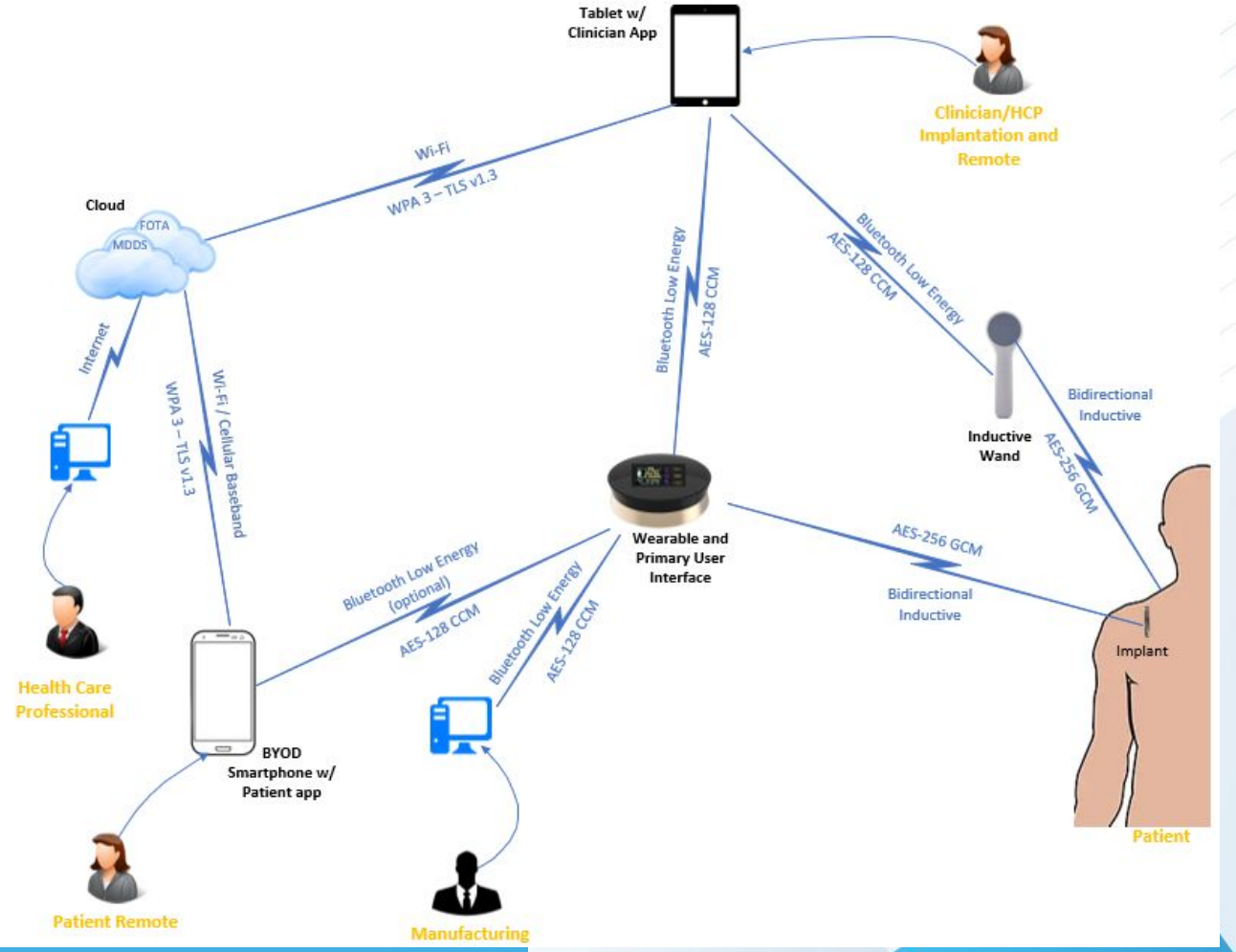


https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

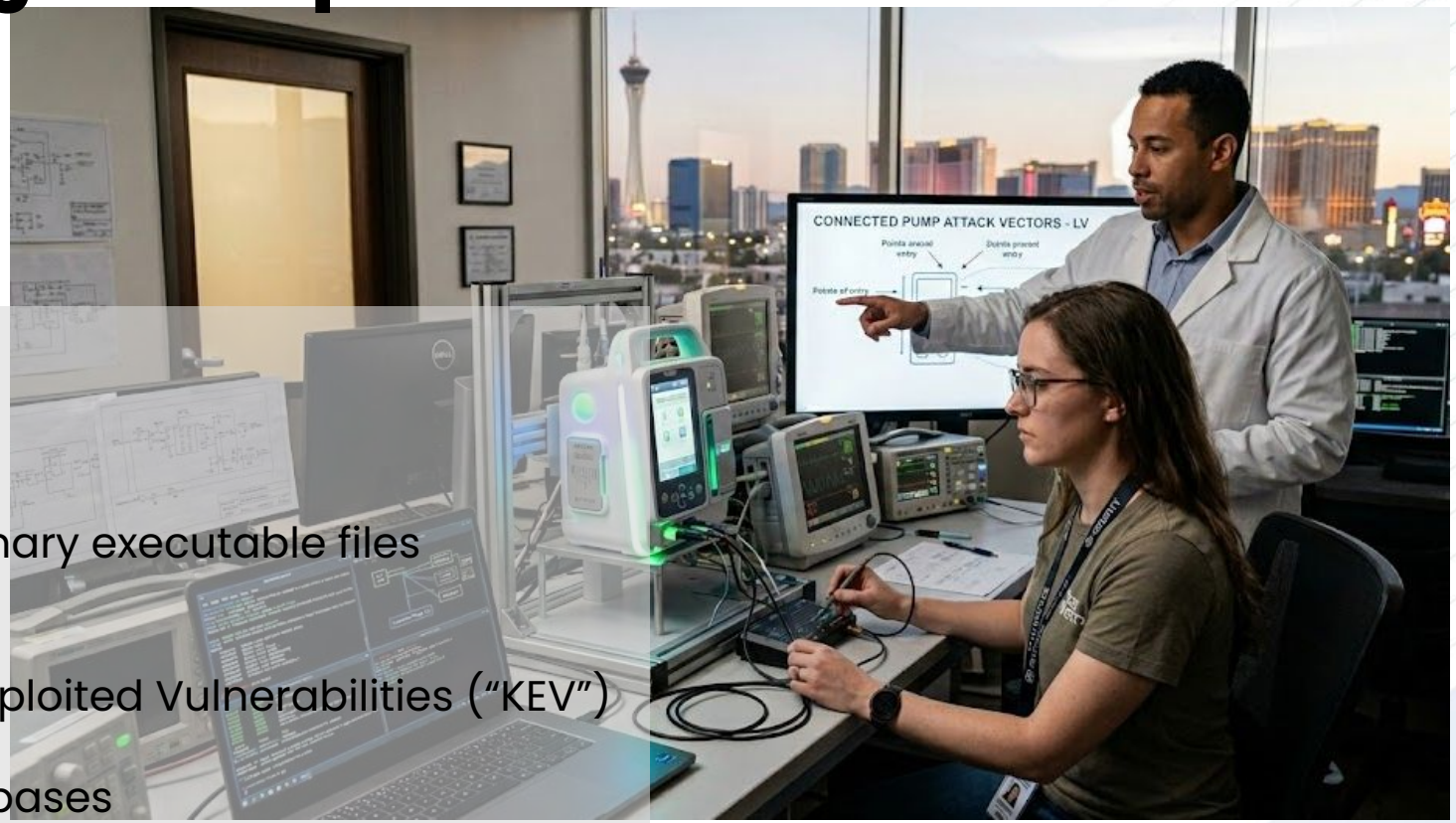
Security Architecture Views

- The Security Architecture Views are to communicate design vulnerabilities and mitigations to the FDA. They consist of diagrams and text to convey your security posture to the FDA

- Global System
- Multi-patient Harm
- Updateability
- Secure use cases



Cybersecurity Testing Development & Post Market



- Malformed user inputs
- Fuzz testing of digital communications
- Attack surface analysis
- Closed box testing of known vulnerabilities
- Software composition analysis ("SCA") of binary executable files
- Static and dynamic code analysis ("SAST")
- Penetration testing
- SBOM monitoring against the CISA Known Exploited Vulnerabilities ("KEV") catalog
- SBOM monitoring against vulnerability databases

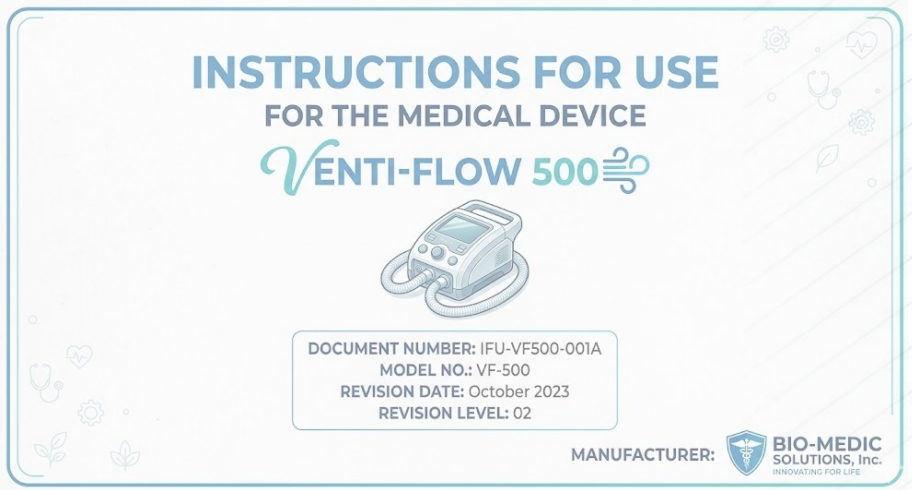
Each of these tests results in a separate report, which, during development, is summarized in the Cybersecurity Testing Report for the FDA's eSTAR.

Sustaining cybersecurity testing should be performed at regular intervals (e.g., **every 3 to 12 months**)

MDR Article 86 PSUR "annual reporting" requires this testing every 12 months!

Cybersecurity Labeling

- Cybersecurity content in the Instructions For Use (“IFU”) :
  - Instructions for performing software updates
  - Device instructions for cybersecurity controls
  - Diagrams that assist in implementing cybersecurity controls
  - Network ports and interfaces that receive/send data
  - Guidance on the supporting infrastructure requirements
  - A human-readable SBOM
  - How the device responds to anomalous conditions
  - The features that protect critical functionality
  - Backup and restore features
  - Methods for retention and recovery of device configuration
  - Secure configuration of shipped devices
  - How forensic evidence is captured
  - If known, the EOS and EOL for each component
  - How to securely decommission the device
  - For each electronic interface
    - The purpose of the electronic interface
    - The anticipated users
    - Specifications (e.g., physiological waveforms, probe type, accuracy, frequency of response, update rate, data rate, bandwidth)
    - Necessary performance and functional requirements
    - List of data attributes exchanged
    - Summary of interface testing to verify interoperability claims
    - Activities suggested to verify safe operation via a representative device
    - All relevant standards and certifications
    - If supported, the method for time synchronization
    - A description of fault tolerance behavior, boundary condition testing, or a fail-safe for critical functions
    - Known limitations, contraindications, precautions, and warnings
    - Recommended connections, settings, or configurations
    - Specific user instructions



Firmware and Software Updates In The Field

- FDA requires that manufacturers should not only build in the ability for devices to be updated/patched, but that manufacturers also plan for the rapid testing and evaluation of devices deployed in the field.
- USB flash drives are not a good approach to updating
- For more on this topic:
  - https://www.ntia.gov/files/ntia/publications/ntia_iot_security_update_framework.pdf

Voluntary Framework for Enhancing Update Process Security

Technical Capabilities and Patching Expectations Working Group

This document was drafted by an open working group convened by the National Telecommunications and Information Administration in a multistakeholder process, including the following individuals and organizations: Arm; Mark Cather, UMBC; Chris Gates, Tim Hahn, IBM; Shrinath Eswarahally, Infineon; Ethan Lucarelli, Inmarsat; Verizon. Others participated, but do not wish to be named.

Top 10 Reasons For a Hold Letter

For the last two years, the FDA has been disclosing the most frequent cybersecurity errors in submissions.

I have arranged these in Top 10 order to reflect what I have personally seen as the most common mistakes.

But to be clear, all of these should be addressed in your submission, no matter the order.

- 10: Attempting to remove connectivity to avoid being classed as a “cyber device”
- 9: Overall lack of documentation clarity
- 8: The manufacturer doesn't provide an assessment of findings and/or describe any changes made as a result of 3rd party Penetration testing.
- 7: Absent or inadequate vulnerability testing (i.e. malformed and unexpected inputs).
- 6: Use of a vulnerability scanner (e.g., Nessus) in place of penetration testing
- 5: Issues with traceability, security risk control mitigations are not adequately traced to security requirements, and testing reports
- 4: Failure to implement adequate security controls
- 3: Cybersecurity risk assessments score security risks using probability
- 2: Use of inappropriate security risk control mitigations or assumptions
- 1: The SBOM is missing the minimum baseline attributes elements ("relationship between components“) and improper formatting

Services Offered By arsMedSecurity

- Fractional / Virtual Chief Product Security Officer
  - Cost-effective alternative staffing option
- Gap Analysis
  - Project gap analysis (DHF review, including all security documentation and activities)
  - QMS Gap Analysis (existing policies/procedures changes and what is missing)
- Project Specific Cybersecurity Assistance (i.e. 510(k) submission focused)
  - Creation of all documents required for the cybersecurity section of the FDA's eSTAR system
  - Review/response for AINN/Hold letter
- Corporate Governance
  - Create missing policies and procedures
  - SOP Alignment with secure development frameworks (IEC 81001-5-1 & NIST 800-218)
  - SOP creation for Coordinated Vulnerability Disclosure and Incident Response
- Post-Market Cybersecurity Testing and Surveillance
  - As required per the FDA’s June 2025 Premarket Guidance
  - Periodic re-performance of cybersecurity testing
  - SBOM monitoring
  - With the results stored in a highly encrypted online folder for customer convenience
- General Cybersecurity Consulting

Contact us at:
sales@arsMedSecurity.com