The (Medical Device) Manufacturer Perspective
Assumptions

• Manufacturers have the information that needs to be shared for software bills of material
  • It’s available in some format as the product is being constructed
  • It’s necessarily there for performing vulnerability monitoring / management

• Manufacturers want to provide information to their customers (transparency goes beyond SBOM)
  • It’s required for collaboration on the reduction of risk
  • It’s the right thing to do, and establishes trust

• Manufacturers understand some of the use cases for software component transparency / bills of material
  • Customer’s proactive risk management
  • Customer’s reactive incident / vulnerability response

• Manufacturers understand some of the requirements / challenges to implement standardized solutions
  • Machine readability
  • Unique software identification
The 3-D Solution Space

Depth (how many items)
- recursion
- snippets
- firmware / hardware
- “all” software components
- attack surface-relevant components

Breadth (how much detail per item)

Time (how often to update)
- at delivery
- major update
- any update
- when patched
- in real time
Nail Down

- Use cases
- Unique software identification
- Available and adaptable frameworks and standards
- The 3-D solution space