IMDRF Stakeholders Forum
March 2021

Medical Device Cybersecurity Update

US FDA & Health Canada Co-Chairs
Presentation Outline

• IMDRF/CYBER WG/N60 Final Guidance, published March 2020
  – Purpose and Scope
  – General Principles
  – Introduction of Legacy and Software Bill of Materials (SBOM)

• New Work Item Extension to expand on and advise on implementation of Legacy and SBOM concepts

• Progress and Planned Milestones
Guidance Purpose & Scope

• Purpose:
  – To provide fundamental concepts and considerations on the general principles and best practices on medical device cybersecurity

• Scope:
  – Considers cybersecurity broadly in the context of medical devices that either contain or composed of software, and not just network connected devices
  – Excludes information security and directly state scope includes medical device safety and performance
  – Includes recommendations to all stakeholders, not just manufacturers
General Principles

1. **Global Harmonization**: Stakeholders are encouraged to harmonize their cybersecurity approaches across the entire life cycle of the medical device.

2. **Total Product Life Cycle (TPLC)**: Risks associated with cybersecurity threats and vulnerabilities should be considered throughout all phases in the life cycle of a medical device.
General Principles cont’d

3. **Information Sharing**: Stakeholders are encouraged to engage in information sharing to increase transparency and collaboration to enable the safe and effective use of medical devices.

4. **Shared Responsibility**: All stakeholders must understand their responsibilities and work closely with other stakeholders to respond to potential cybersecurity risks and threats.
Two Concepts introduced in N60

• **Legacy Medical Device**: medical devices that cannot be reasonably protected (via updates, and/or compensating controls) against current cybersecurity threats.

• **Software Bill of Materials (SBOM)**: a list identifying each software component by its name, origin, version and build of any commercial, open source, or off-the-shelf software components which are included in the medical device.
Legacy Conceptual Framework

• N60 defined a conceptual framework to define the responsibilities between manufacturer and customer throughout the total product life cycle.

• N60 emphasizes that device age is not a sole determinant of legacy status.

• N60 provides some recommendations to both the manufacturer and the customer throughout the different stages of the total product life cycle.
Legacy Device Conceptual Framework as a Function of TPLC

Cybersecurity and the Total Product Life Cycle

*Medical Device Manufacturer (MDM) follows regional guidance for medical device responsibilities, support levels may vary and as agreed upon with customers.
Software Bill of Materials (SBOM)

- SBOMs can enable device operators to manage their assets and related risks.

- Device operators can use the SBOM to facilitate work with the device manufacturer in identifying software that may have vulnerabilities, update requirements, and performing appropriate security risk management.

- The SBOM can help inform purchasing decisions by providing prospective buyers with visibility into the components used in applications and determining potential security risk.

- Manufacturers should leverage industry best practices for the format, syntax and markup used for deployment of the SBOM.
New Work Item Extension

How should stakeholders implement and operationalize:

• SBOM
• Legacy conceptual framework
New Work Item Extension

**Goal:** To increase international alignment and improved safety and security by:

1. Addressing implementation of SBOM, as well as transparency in the use and support of third-party software;
   - Topics may include: lessons learned regarding construction, granularity, distribution, use, and support of third-party software including SBOM.

2. Operationalizing the legacy device conceptual framework articulated in the N60 document in a related, but separate document.
   - Topics may include: additional definitions, legacy device best practices, post-market vulnerability management, economic and regulatory incentives, etc.
Progress and Planned Milestones

- February 3, 2021: New Work Kickoff Meeting
- April 2021: Final Document Outline
- April-October 2021: WG Meetings every two weeks
- October/November: 4-day WG Meeting
- February 2022: Submission of draft to IMDRF MC
- April 2022: Public Consultation*
- April-October 2022: WG Meetings
- October/November 2022: 4-day WG Meeting
- March 2023: Publish Final Document(s)*

* Pending IMDRF MC Approval
Thank you

• IMDRF Cybersecurity WG
• IMDRF Management Committee
• IMDRF Secretariat
• IMDRF Webmaster