SELECTION OF CYBERSECURITY-RELATED STANDARDS IN DEVELOPMENT FOR MEDICAL DEVICES

I. ISO/IEC

ISO/IEC 81001-1 Health software and health IT systems safety, effectiveness, and security – Part 1: Foundational principles, concepts and terms (Current status: Committee Draft 2)

Focus on the entire lifecycle of health software and systems, from concept to decommission. Security is one of the foundational elements. As part of the overall "cradle to grave" approach, this standard is taking an approach to also focus on the importance of information transfer as a product moves from manufacturer to implementer & integrator to user. This information would include information regarding risk, usability, configuration, and other important information that is necessary for stakeholders to transfer and maintain ownership of the product. Another focus of this standard is to identify and define common terms to harmonize the definitions used across the lifecycle where possible.

IEC 80001-5-1 Safety, effectiveness, and security in the implementation and use of connected medical devices or connected health software – Part 5: Security – Part 5-1: Activities in the product lifecycle (Current status: Approved project, kick-off Feb 4-6, 2019)

This standard is at an early stage of development. The current plan is to model this standard after IEC 62304, approaching the health software development lifecycle standard from a security-specific perspective. Current plan is to cover both product development and use lifecycles. Standard number may be modified in the future. This standard will focus on process.

IEC 60601-4-5 Guidance and interpretation – Safety related technical security specifications for medical devices (Call for Experts in IEC SC 62A)

As compared to IEC 80001-5-1, this standard will focus on the controls specific to the security of medical devices.

IEC 62304 Medical device software – Software life cycle processes (Current status: under revision)

IEC 62304 is a foundational standard for software development lifecycle for medical devices. The current revision is proposing to include certain aspects of security to segment the standard and provide clarity for users.

II. AAMI

AAMI TIR97/Ed. 1, Principles for medical device security – Post-market security management for device manufacturers (Current status: completing comment resolution process)

This technical information report offers detailed guidance on managing medical device security in a postmarket stage, including considerations for developing security policies and program administration, design features for postmarket security, installation and configuration, and retirement/obsolescence considerations.

AAMI SW96/Ed. 1, Medical Devices – Application of security risk management to medical devices (Current status: approved project, on hold while group finishes AAMI TIR 97)

SELECTION OF CYBERSECURITY-RELATED STANDARDS IN DEVELOPMENT FOR MEDICAL DEVICES

A standard to be developed based on AAMI TIR 57, a current medical device security risk management technical information report.