P2621.3

Submitter Email: dklonoff@diabetestechnology.org
Type of Project: New IEEE Standard
Project Request Type: Initiation / New
PAR Request Date: 14 Jan 2020
PAR Approval Date: 04 Mar 2020
PAR Expiration Date: 31 Dec 2024
PAR Status: Active

1.1 Project Number: P2621.3
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Project Title: Standard for Wireless Diabetes Device Security Assurance: Guidance for Mobile Devices

3.1 Working Group: Healthcare Device Security Assurance Working Group(EMB/Stds Com/HDSecWG)
3.1.1 Contact Information for Working Group Chair:
Name: David Klonoff
Email Address: dklonoff@diabetestechnology.org
3.1.2 Contact Information for Working Group Vice Chair:
None
3.2 Society and Committee: IEEE Engineering in Medicine and Biology Society/Standards Committee(EMB/Stds Com)
3.2.1 Contact Information for Standards Committee Chair:
Name: Carole Carey
Email Address: c.carey@ieee.org
3.2.2 Contact Information for Standards Committee Vice Chair:
Name: Hasan Al-Nashash
Email Address: hnashash@aus.edu
3.2.3 Contact Information for Standards Representative:
Name: Carole Carey
Email Address: c.carey@ieee.org

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE SA for Initial Standards Committee Ballot: Oct 2020
4.3 Projected Completion Date for Submittal to RevCom: Apr 2021

5.1 Approximate number of people expected to be actively involved in the development of this project: 25
5.2 Scope of proposed standard: This standard provides instruction for the safe use of consumer mobile devices (CMDs) in the control of
diabetes-related medical devices, including:
1. The safe use of CMDs in both "open loop" and "closed loop" diabetes control solutions.
2. Instruction for the creation of security targets that leverage CMDs, with differentiated emphasis for security targets intended to meet the enhanced-basic and moderate assurance levels, as defined in other parts of this standard.
3. Instruction for leveraging CMDs in control solutions that have stringent real-time and high-availability (of the connected diabetes device (CDD) solution and/or its enclosing personal area network) requirements.

5.3 Is the completion of this standard contingent upon the completion of another standard? No
5.4 Purpose: The purpose of this standard is to define requirements for the use of mobile devices in diabetes contexts, as deemed necessary and sufficient by an appropriate set of stakeholders. These requirements are intended to be used within an evaluation program, as defined in the first part of this standard.
5.5 Need for the Project: The need to assure medical device functionality and safety has become more challenging with the growing use of wireless and Internet-connected devices. There is significantly increased use of off-the-shelf consumer mobile devices (CMDs), (e.g. smartphones) in medical contexts.
In order to realize the potential beneficial uses of consumer digital technology, the medical community, including

device manufacturers, regulators, caregivers, and patients must be aware of the risks associated with the use of
CMDs and apps in these contexts and follow appropriate regulatory, developmental, lifecycle management, and usage guidelines to ensure that proper functionality and safety are maintained.
5.6 Stakeholders for the Standard: Device manufacturers, clinicians, regulators, certification bodies, independent cybersecurity/privacy experts, healthcare facilitators, test labs, software developers, and patients/consumers.

6.1 Intellectual Property

6.1.1 Is the Standards Committee aware of any copyright permissions needed for this project? Yes

Explanation: The basis of this standards will be the Diabetes Technology Society standard DTMoSt.

6.1.2 Is the Standards Committee aware of possible registration activity related to this project? No

---

7.1 Are there other standards or projects with a similar scope? Yes

Explanation: UL 2900

The UL 2900 series of standards consists of the following parts, under the general title "Standard for Software Cybersecurity for Network-Connectable Devices":
Part 1: General Requirements for Network-Connectable Devices
Part 2-1: Particular Requirements for Healthcare Systems
Part 2-2: Particular Requirements for Industrial Control Systems
Part 3: General Requirements for the Organization and Product Development Security Lifecycle Processes for Network-Connectable Devices

7.1.1 Standards Committee Organization: UL

Project/Standard Number: UL2900

Project/Standard Date:

Project/Standard Title: Cybersecurity for Network Connected Diabetes Devices

7.2 Is it the intent to develop this document jointly with another organization? Yes

7.2.1 Organization: Underwriter Laboratories

Technical Committee Name: N/A

Technical Committee Number:

8.1 Additional Explanatory Notes : These standards were previously under one standard (P2721) but have now been separated into three separate but related standards:
2621.1 Defines a framework for a connected electronic product security evaluation program.
2621.2 Defines the security requirements, which compose a Protection Profile, for connected diabetes devices.
2621.3 Provides instruction for the safe use of consumer mobile devices in the control of diabetes-related medical devices.
IEEE and UL have signed an MOU for joint development
2.1 and 5.2: The connected devices used in diabetes might have different properties and different vulnerabilities than connected devices used for other diseases. We intend to build this standard for diabetes first. This standard might be useful as a template for connected devices for other diseases in the future. We feel that this project is more likely to
be successful if we focus on diabetes devices rather than devices for all types of health conditions.