IEEE MEDICAL DEVICE CYBERSECURITY STANDARD & CERTIFICATION PROGRAM
INDUSTRY LED DEVELOPMENT

• **Standards Approved** – March 2021, IEEE Board approval
• **Test Plan approved** – December 2022, IEEE Certification Advisory Committee approval
• **Pilot Testing** – Started in Q1 2023, **first certifications expected in Q1 2024**

• **Strong industry support** – 17+ companies including major security vendors
  ▪ Standards and Cert. Program developed under the leadership of Dr. David Klonoff (DTS) and Dave Kleidermacher (Google)

• **Strong regulatory support** – standard already included in FDA’s catalog of standards

![Abbott](#) ![ASCENDIA Diabetes Care](#) ![BD](#) ![THIRDDAY](#) ![DIABETES TECHNOLOGY SOCIETY](#) ![EOFLOW](#)
![FDA](#) ![Google](#) ![Lifescan](#) ![INTERTEK](#) ![medcrypt](#) ![Roche](#) ![Diagnostics](#)

![IEEE SA](#) ![SANSUM DIABETES RESEARCH INSTITUTE](#) ![SAMSUNG](#) ![SAMSUNG RESEARCH AMERICA](#)
CYBERSECURITY ECOSYSTEM FOR INDUSTRY

- FDA is setting the bar – cybersecurity capabilities now required by LAW

Current Scope of the IEEE Certification Program: Connected diabetes devices
  - BGM, CGM, Insulin Pump, Insulin Pen, Closed Loop System/AID system,…

Future Scope: All medical devices
  - Work on extending the scope to other medical devices will start this year
  - IEEE Solution Partner Program (under development)

Comprehensive Security Evaluation Program

The bottom line: MDM should expect a smooth regulatory submission process!
Example Assets to Protect

Data

Device Processes

Communications

MEDICAL DEVICE

Example Threat Agents

Attackers

Unauthorized Users

Privileged Users

Developers

Adverse Impact on Assets

Security Objectives for Device

Assumptions

Security Objectives for Environment

USING ISO/IEC 15408 TO DEVELOP IEEE 2621

Security Objectives for Environment

Assumptions

Security Objectives for Device

Example Assets to Protect

Example Threat Agents
IEEE SECURITY TARGET FOR MEDICAL DEVICES

Security Objectives for Device

Security Objectives for Environment

Assumptions

Security Target

Select Security Functional Requirements (SFRs) to satisfy security objectives

ISO 15408 (Common Criteria)

Select Security Assurance Requirements based on several factors:

- Risks associated with compromise of the assets
- Technical feasibility
- Likely development and evaluation costs
- Required timescales for development and evaluation of the CMD
- Perceived market and/or regulatory requirements
- All identified dependencies of SFRs on SARs
IEEE 2621 MULTI-PART STANDARDS

- Approved IEEE standards as of March 2022
  - The IEEE 2621 standard uses the Common Criteria (CC) program as a basis for its security functional and assurance requirements; conforms to the requirements of ISO 15408-1, 2, 3
  - Designed to be applicable to all medical devices, currently focused on connected diabetes devices
    - Examples: BGM, CGM, Insulin Pump, Insulin Pen, Closed Loop System/AID system,…

- IEEE 2621.1 - Framework for a connected electronic product security evaluation program
  - Assurance Levels:
    - Basic Assurance Package - Manufacturer self-test
    - Moderate - Testing by authorized test lab. Represents advanced security.
  - Lab Accreditation, Certification Criteria and Assurance Maintenance

- IEEE 2621.2 - Security requirements and protection profile
  - Security threats/risks and functional requirements that counter these threats
  - Protection profile

- IEEE 2621.3 - Guidance for mobile devices in diabetes control contexts
  - Ex. Usage of applications on smartphones to control insulin injection levels
IEEE STANDARD EVALUATION REPORT

Manufacturer Submission to Test Lab

- Security Target documentation
- Product security flaw remediation process(es)
- An attestation signed by a Manufacturer authority

Evaluation Result: Standard Report submitted to IEEE

Work Unit | Evaluation Requirement | Expected Results | Status | Rationale/Reference(s)/Comment(s) | Result
---|---|---|---|---|---
ASE_SPD.1-1 | The Evaluator shall check that the security problem definition describes the threats. | Threat T_NETWORK identified correctly | TBD | TBD | TBD
 | Threat T_PHYSICAL identified correctly | TBD |
 | Threat T_BAD_SOFTWARE identified correctly | TBD |
 | Threat T_BAD_P2P identified correctly | TBD |
 | Threat T_WEAK_CRYPTO identified correctly | TBD |

ASE_SPD.1-2 | The Evaluator shall examine the security problem definition to determine that all threats described in terms of (1) a threat agent | if ASE_SPD.1-1 is satisfied, then this work activity too is satisfied | TBD |
 | The Evaluator shall examine the security problem definition to determine that all threats described in terms of (2) an asset | TBD |
 | The Evaluator shall examine the security problem definition to determine that all threats described in terms of (3) an adverse action | TBD |

Result: Pass, Fail, N/A, TBD
IEEE certification will help you smooth out the FDA submission process and will increase chances of product approval.

- Test Plans based on the 2621 standard and Inspection Checklists on AAMI TIR57 and IEC 8000-1-5
- Authorized Test Labs, Certificates, Registry
- Solution Partner Program (under development)
- Extension to other medical devices will start after Pilot completion

Contact IEEE if you are interested in any of the above: medcyber@ieee.org

IEEE Conformity Assessment Program (ICAP)
Thank You!

QUESTIONS?

IEEE CONFORMITY ASSESSMENT PROGRAM
TED OSINSKI
PROG. MGR., CONFORMITY ASSESSMENT
TED.OSINSKI@IEEE.ORG

IEEE CONFORMITY ASSESSMENT PROGRAM
RAVI SUBRAMANIAM
DIRECTOR, SA BUSINESS DEVELOPMENT & CONFORMITY ASSESSMENT
R.SUBRAMANIAM@IEEE.ORG

medcyber@ieee.org