Cybersecurity Compliance: Global Considerations for Healthcare

NOVA LEAH

Michelle Jump, VP of Cyber Program Initiatives, Nova Leah

NOVA LEAH
SELECTEVIDENCE

- VP of Cyber Program Initiatives at Nova Leah
  - Strategic leadership, training, and education for SelectEvidence
- MS Regulatory Science, MS Biotechnology
- Author and Project Lead:
  - ISO/IEC 81001 Project Lead
  - Task Group Lead: NTIA Software Transparency
  - Co-Chair AAMI Software Working Group
  - U.S. Technical Expert ISO 80001-5-1
- Member
  - ISO/TC 215 JWG 7, JWG 3
  - AAMI Device Security, Interoperability, Software, Wireless
  - CVSS Medical Device Rubric

About me…

NOVA LEAH
SELECTEVIDENCE

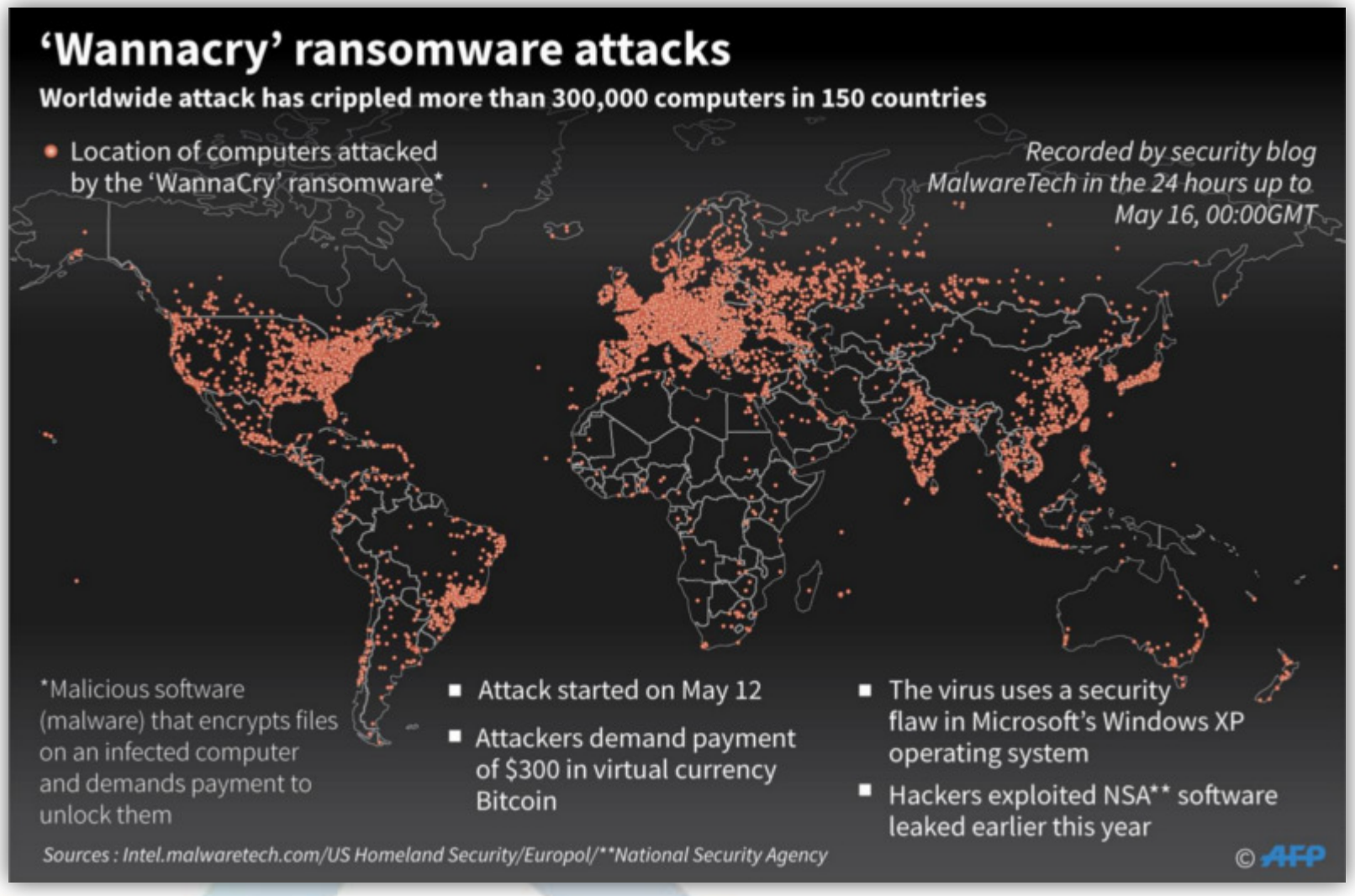
NOVA LEAH
SELECTEVIDENCE

Agenda

I. Global Impact: Drivers for Compliance
II. IMDRF
III. Europe
IV. China
V. Additional Country-Specific Trends
VI. Common Thread: Identifying Themes

NOVA LEAH
SELECTEVIDENCE

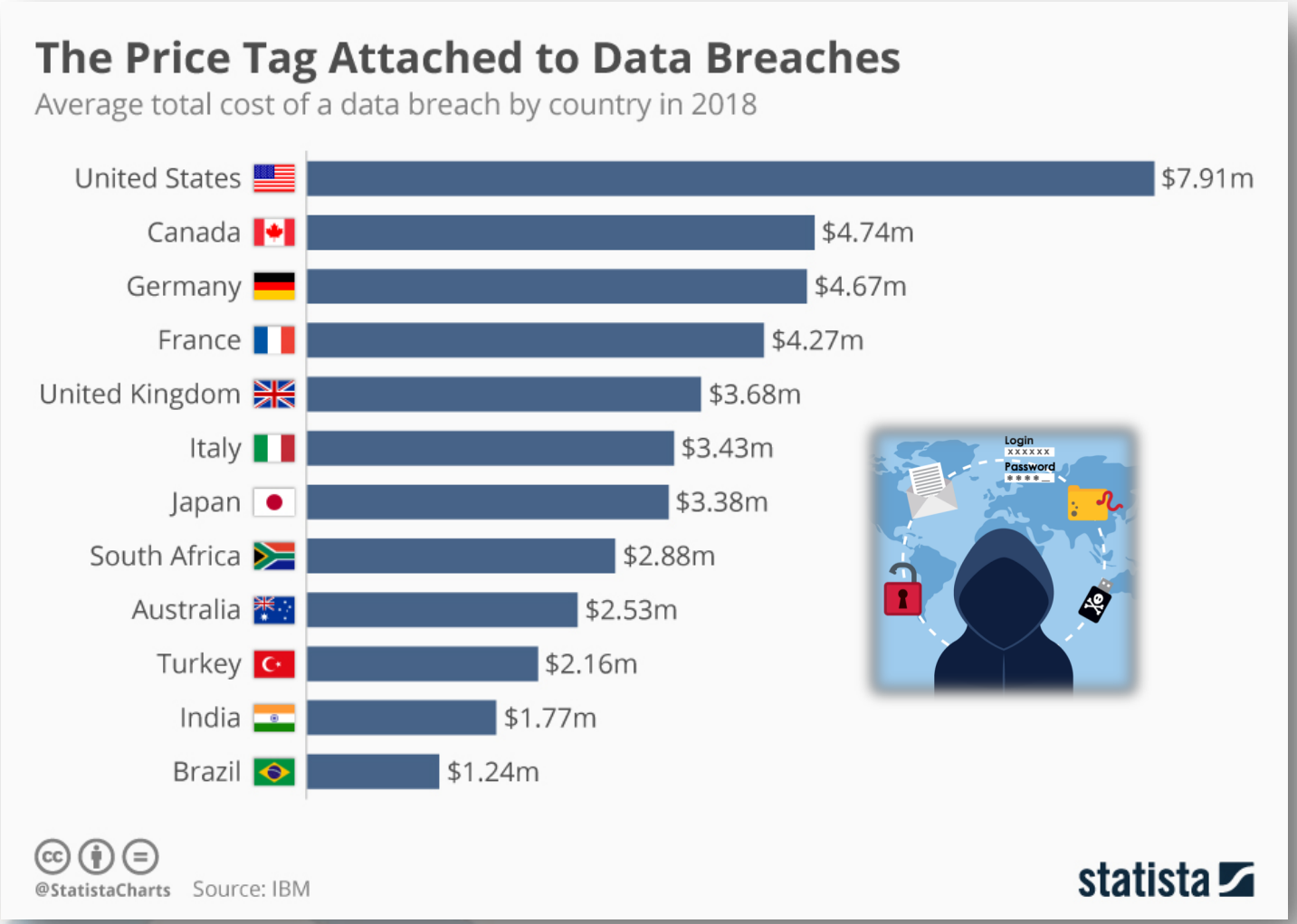
Wannacry: Catalyst for Action



http://www.visualcapitalist.com/watch-cyberwar-live-map/

NOVA LEAH
SELECTEVIDENCE

The Cost is Significant



https://www.statista.com/chart/9918/the-price-tag-attached-to-data-breaches/

NOVA LEAH
SELECTEVIDENCE

IMDRF International Medical Device Regulators Forum

New Cybersecurity Working Group:

- Co-Chaired by U.S and Canada
- Plans to publish an international guidance document on:
  - Definition such as privacy, exploit, threat, vulnerability
  - Outline stakeholder shared responsibilities
  - Global coordinated Vulnerability Disclosure policies
  - Inform SDOs to produce "regulatory-grade" standards – validated methodologies and measurements for success
- Due Sept 2019

Europe

NOVA LEAH
SELECTEVIDENCE

Cybersecurity in Europe

- EU Cybersecurity Act – proposal May 29, 2018
  - European Union Agency for Network and Information Security (**ENISA**) - now permanent agency in EU
  - Helping to align with goal of "Single Digital Market" strategy in EU
- **Efforts underway to provide specific expectations for medical devices**
- Germany released specific set of requirements[1] for network-compatible medical devices (in German)

[1]Bundesamt für Sicherheit in der Informationstechnik, 'Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte'. 02-May-2018

NOVA LEAH
SELECTEV/DENCE

Europe:
Baseline Security Recommendations for IOT

Europe:
Baseline Security Recommendations for IOT
(103 pgs)

NOVA LEAH
SELECTEVIDENCE

Europe:
Baseline Security Recommendations for IOT

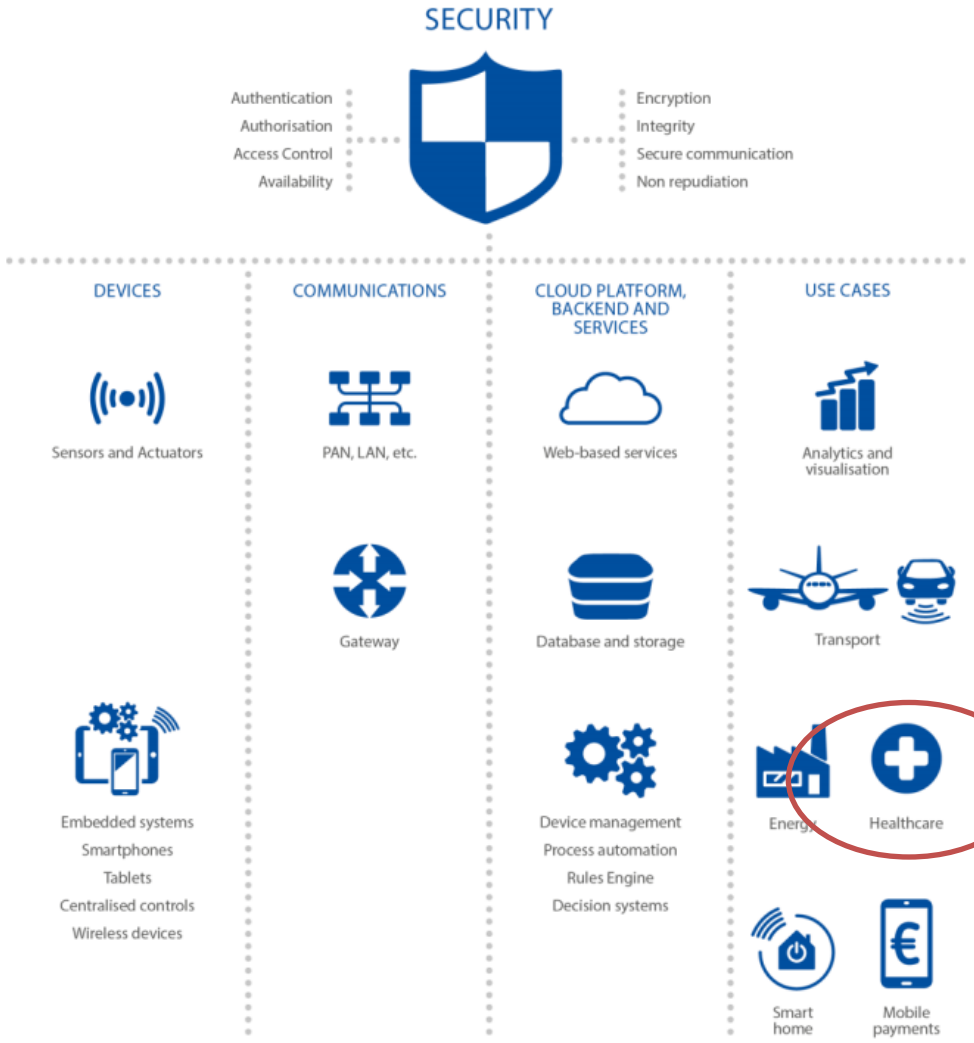
Goal

- Elaborate **baseline cybersecurity recommendations** for IoT with a focus on **Critical Information Infrastructures**, which encompass facilities, networks, services and physical and information technology equipment.
- Critical: their **destruction or disruption could bring about major consequences for the health, safety and economic wellbeing of citizens**

Key Points:

- The recommendations are partially intended to help companies meet new **European data privacy requirements** under the General Data Protection Regulation, or GDPR.
- The European report **cites US FDA guidance** regarding medical device cybersecurity principles and recommendations.

Europe: Baseline Security Recommendations for IOT



Healthcare is one of industries

Figure 4: IoT High-level reference model

NOVA LEAH
SELECTEV/DENCE

Europe:
Baseline Security Recommendations for IOT

- Summary of Document Content:
  - Section 1: Introductory Material
  - Section 2: Description of IoT Paradigm
  - Section 3: Educational content on Threats and Risk Analysis
  - Section 4: Security Best Practices
  - Section 5: Gaps
  - Section 6: Security Recommendations
  - Annexes

NOVA LEAH
SELECTEV/DENCE

Europe:
Section 4: Security measures and good practices

1. Policies (PS)
2. Organizational, People and Process measures (OP)
3. Technical Measures (TM)

Example:

4.3.5 System safety and reliability

- GP-TM-15: Design with system and operational disruption in mind, preventing the system from causing an unacceptable risk of injury or physical damage.
- GP-TM-16: Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.
- GP-TM-17: Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems.

NOVA LEAH
SELECTEV/DENCE

Europe:
Section 5: Gap Analysis

6 Different Gaps Identified - Example: Insecure

5.3 Gap 3: Insecure design and/or development

There have been several studies on design and development concerns related to IoT security[77,78,79,80] . During the interviews engaged within the context of this report we validated the findings of these studies and in this respect the following issues seem particularly significant in the context of IoT design and development:

- No defence-in-depth strategy during the design of the system, such as a secure boot process, isolation of a Trusted Computing Base, limitation of the number of open ports, self-protection, etc.
- No security-by-design or privacy-by-design. In some cases, information is exchanged with a third-party, and it should be ensured that not more information than strictly needed is exported outside of the IoT environment.
- Lack of communication protection, on internal as well as external interfaces.
- Lack of strong authentication and authorisation:
  - No validation or signing of firmware updates,
  - Software updates without server authentication and file trust verification,
  - No secure boot mechanisms.
- Lack of hardening:
  - No data execution prevention or attack mitigation technologies used on the firmware,

NOVA LEAH
SELECTEVIDENCE

Europe:
Annex A: Security Measures/Good Practices

- Categorized into:
  1. Security by Design
  2. Privacy by Design
  3. Asset Management
  4. Risk and Threat Identification and Assessment
  5. Hardware security
  6. Trust and Integrity Management
  7. Strong Default Security and Privacy
  8. Data Protection and Compliance
  9. System Safety and Reliability
  10. Secure Software/Firmware Updates
  11. Authentication
  12. Authorization
  13. Access Control
  14. Cryptography
  15. Secure and Trusted Communication
  16. Secure Interfaces and Network Services
  17. Secure Input and output Handling
  18. Logging
  19. Monitoring and Auditing
  20. End of Life Support
  21. Proven Solutions
  22. Management of Security Vulnerabilities and/or incidents
  23. Human Resource Security Training and Awareness
  24. Third Party Relationships

24 Categories of Detailed Security Measures (18 pages of Security

NOVA LEAH
SELECTEVIDENCE

Europe:
Baseline Security Recommendations for IOT

- Annex C: Security Standards and References

AUTHOR	TITLE	REFERENCE
1. EU Initiatives		
DG CONNECT commissioned study, authored by IDC Italia S.r.L and TXT e-solutions S.p.A.	Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination	https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
European Commission	Digitising European Industry Reaping the full benefits of a Digital Single Market (COM(2016) 180 final)	https://ec.europa.eu/digital-single-market/en/digitising-european-industry
		http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
	Building A European Data Economy	http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41205
		http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41247
	ICT Standardisation Priorities for the Digital Single Market	https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market
		http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15265
	Advancing the Internet of Things in Europe	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110
	H2020	https://ec.europa.eu/programmes/horizon2020/
	EU cybersecurity initiatives	http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf
Article 29 Data Protection Working Party	Opinion 8/2014 on the on Recent Developments on the Internet of Things	http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
IERC European Research Cluster on the Internet of Things	IoT Governance, Privacy and Security Issues - IERC Position Paper	http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf
EC Alliance for Internet of Things Innovation (AIOTI)	AIOTI WG04: Report on Policy Issues	https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf
	AIOTI WG03: SmartM2M; IoT Standards landscape and future evolutions (October 2016 with the contribution of ETSI)	https://aioti-space.org/wp-content/uploads/2017/03/tr_103375v010101p-Standards-landscape-and-future-evolutions.pdf

NOVA LEAH
SELECTEV/DENCE

Europe: Baseline Security Recommendations for IOT

- Annex D: Description of IoT Security Incidents

SECURITY INCIDENT	DATE	DESCRIPTION
TrackingPoint's smart sniper rifle hack (demonstration)	July 29, 2015	Security researchers Runa Sandvik and Michael Auger have developed a set of techniques that could allow an attacker to exploit vulnerabilities in the software of a US$13,000 TrackingPoint self-aiming rifle via its Wi-Fi connection. The attacker could then compromise the scope's targeting system, preventing the gun from firing or even causing it to miss the intended target, hitting another one[88].
VTech Toymaker data breach	November 8, 2015	A cyber-attack on digital toymaker VTech Holdings exposed the data of 6.4 million children and 4.9 million adults. The personal information stolen was not encrypted, and it included names, email addresses, passwords, secret questions and answers for password retrieval, IP addresses, postal addresses, download histories, chat logs, and children's names, photos, genders and birth dates[89].
Mirai - DDoS on OVH hosting provider	September 19, 2016	Mirai gathered a botnet made up of more than one million hacked IoT devices, mostly DVRs and CCTV cameras, which were infected through their Telnet port. The French hosting company OVH is believed to be the first to have suffered a DDoS attack coming from the Mirai botnet, which was reported to have peaked at 1 Tbps, one of the largest recorded in history in terms of volume[90].
Mirai - DDoS on "Krebs on Security" website	September 20, 2016	Just a day after the attack against OVH, the Mirai botnet conducts a DDoS attack on "Krebs on Security" website that surpassed 620 Gbps of traffic, making it also one of the largest recorded in history in terms of volume[90].

China

NOVA LEAH
SELECTEVIDENCE

New CFDA Cybersecurity Expectations

Timeline

- **11-7-16:** China Cybersecurity Law enacted
- **1-20-17:** CFDA issued updates on to implement the CSL in the administration of medical devices
- **1-1-18:** MDM required to register networked medical devices with the CFDA
  - Assessed by CFDA for their **cybersecurity protection status***
  - Companies conduct a **self-assessment** of the relevant cybersecurity protection standards or measures
  - **Not mandatory** obligations but failure may cause delay in registrations.

*per *Principles on Guiding Technology Examination of Medical Device Cybersecurity Registration*

NOVA LEAH
SELECTEVIDENCE

Scope – Qualified Devices

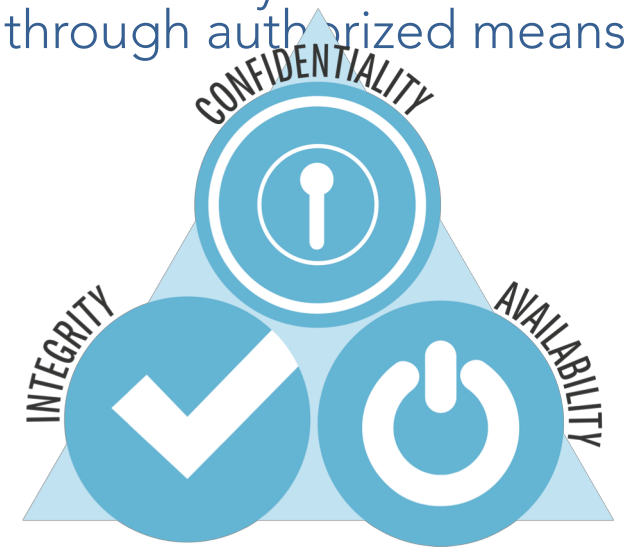
- The latest cybersecurity guidelines published by CFDA this year covers Type 2 and Type 3 devices that can be
  (1) **connected** for data exchanges or remote control or
  (2) those that use **storage media** to exchange information.

(CFDA is likely to make these measures mandatory in the near future.)

NOVA LEAH
SELECTEVIDENCE

Focus of CFDA

- **Follow the CIA Triad Model:** Confidentiality, Integrity and Availability (CIA)
  - Confidentiality the data can only be accessed by authorized users within an authorized timeframe through authorized means,
  - Integrity the data must be accurate, comprehensive and cannot be altered without authorization
  - Availability the data must be accessible and utilized as expected.
  - **Confidentiality**: the data can only be accessed by authorized users within an authorized timeframe through authorized means
- **Focus on entire process:** data generation to data consumption (from "making" to "using" data)



NOVA LEAH
SELECTEVIDENCE

Recommended Approach

Approach

- Consider **entire lifecycle**
- consider **all** data types such as patient's **personal information** or **device's own data** from its operations.
- Focus on: data technology in **access, encryption, protection,** and **response mechanisms.**
- Show control of the embedded software with adequate **monitoring, upgrade, and security protection** with tracking mechanism.

Expectations

- submit a **standalone cybersecurity description file** and a **cybersecurity instruction manual**.
- For "**major cybersecurity update**" affecting the safety or effectiveness of the Qualified Devices after the initial registration, the applicant is **required to file a revised application with the CFDA.**

NOVA LEAH
SELECTEVIDENCE

Review Factors

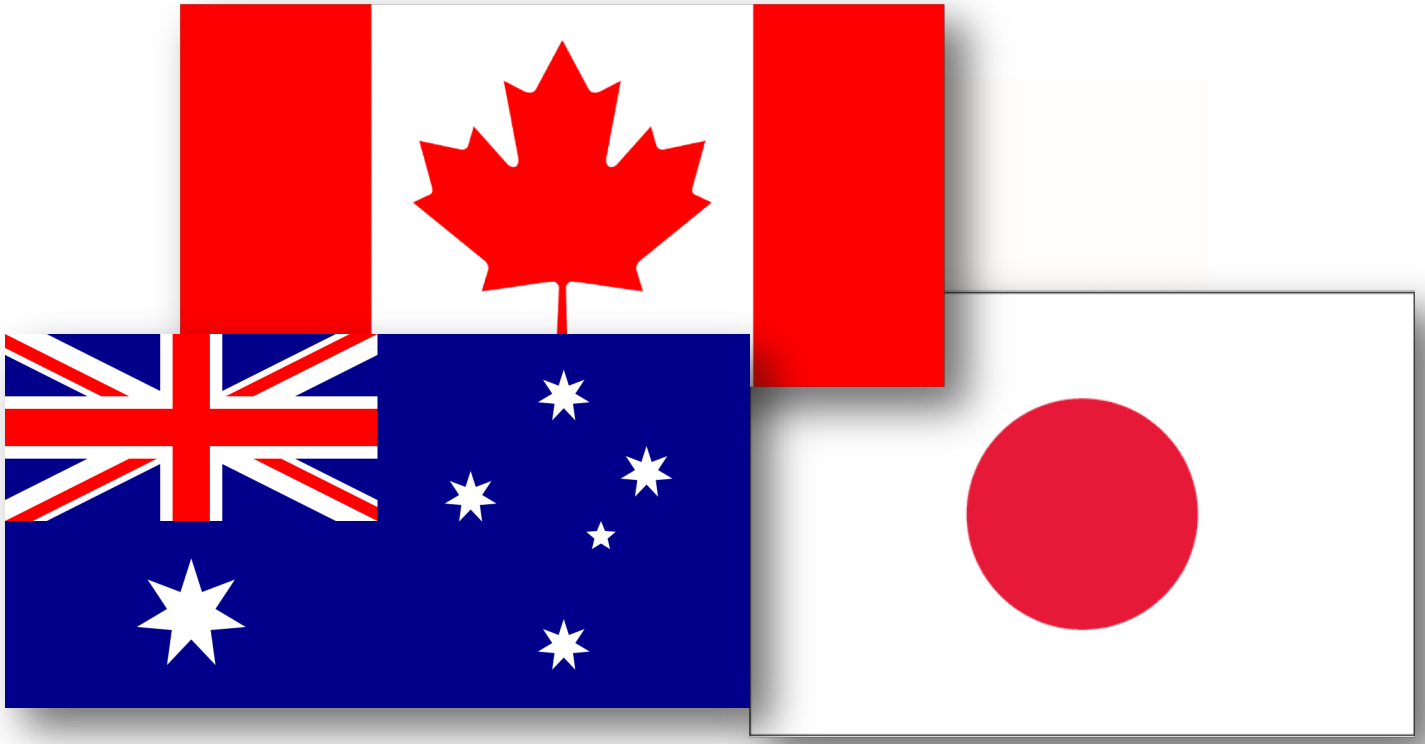
Consistent expectations with other regions and industry overall

When reviewing the product cybersecurity registration process, the CFDA will consider:

- **Data**: the data on the Qualified Devices can be categorized as personal data and equipment data. Different protection measures should be adopted depending on the type of data and the transmission method. Personal data usually warrants enhanced protection and relevant personal privacy protection rules should be followed.

- **Technology**: different cybersecurity protection technology can be utilized. The applicant may follow various international and national standards to build up their cybersecurity protection capability.

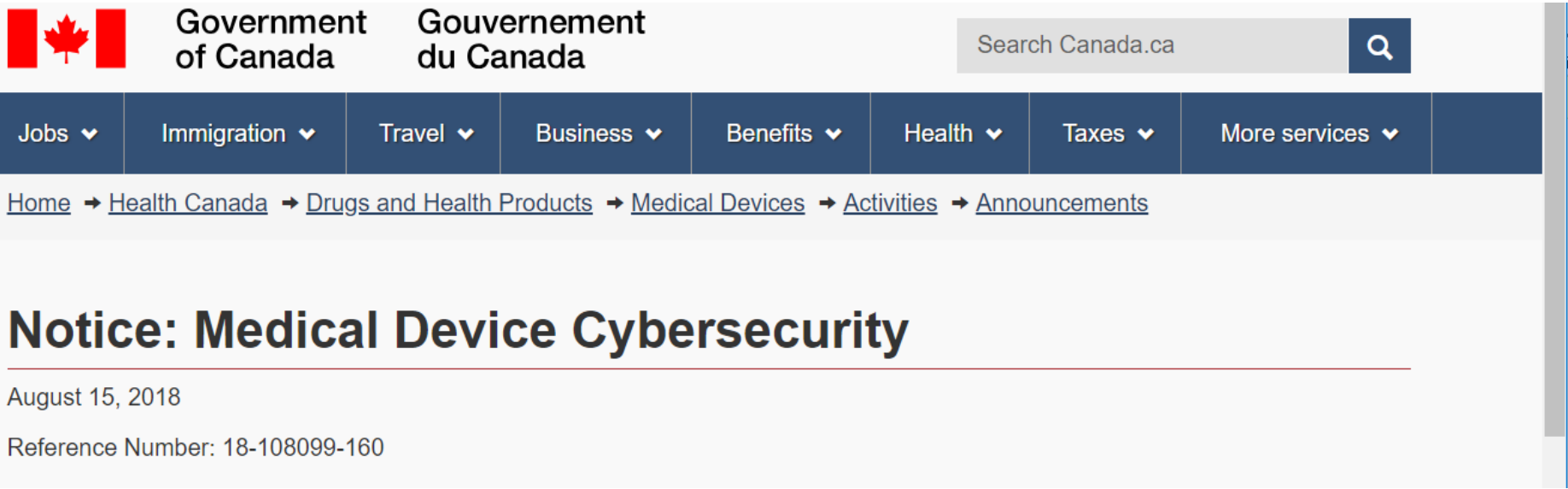
- **Off-the-shelf software**: the applicant is expected to pay close attention to the cybersecurity risks associated with off-the-shell software and adopt relevant maintenance procedures, as well as notify users of relevant information in a timely manner.



Developing Guidance

Other Country-Specific Regulatory Trends in Cyber

Canada



- In fall 2018 Health Canada will:
  - seek input on its approach to medical device cybersecurity from the Scientific Advisory Committee on Digital Health Technologies (SAC-DHT), and
  - publish a draft guidance document on the pre-market requirements for the cybersecurity of medical devices for comment to the Health Canada website.

https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-cybersecurity.html

NOVA LEAH
SELECTEVIDENCE

Japan

- Guidance for Ensuring Cybersecurity in Medical Devices (Notification No. 0724-1, July 24, 2018)
- Primary focus on risk management
  - Cybersecurity is now considered a foreseeable hazard
- Dual approach
  - Both technical controls and procedural protection
- Similar to US FDA: shared responsibility

NOVA LEAH
SELECTEVIDENCE

Australia

Guidance will inform developers, sponsors, and users

Australian Government
Department of Health
Therapeutic Goods Administration

Search TGA

Home | Safety information | Consumers | Health professionals | Industry | About the TGA | News room

News room

- News & public notices
  - Latest news & updates
  - Media releases & statements
  - Behind the news
  - **Newsletters & articles**
  - Subscribe to updates
  - TGA tenders
- Consultations & reviews
- Events, training & presentations

Home › News room › News & public notices › Newsletters & articles

A- A+ Share

Research: Software as a Medical Device and Cyber Security for Medical Devices

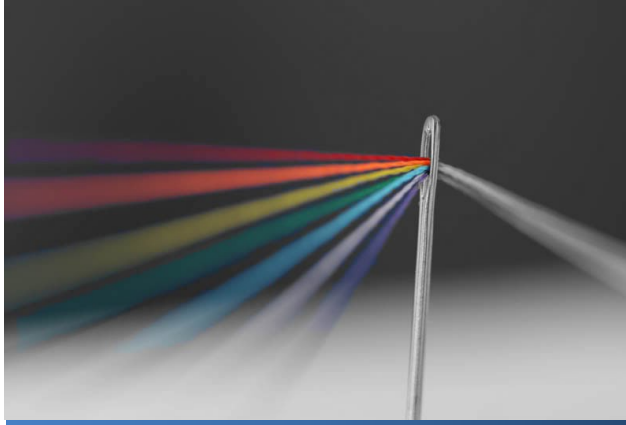
7 August 2018

Globally, regulators of therapeutic goods are faced with numerous challenges concerning emerging medical device technology. The Therapeutic Goods Administration (TGA) recognises that, to continue providing a clear regulatory environment for medical devices in Australia, it is essential that we engage with the medical devices ecosystem during the development of new regulatory recommendations and guidelines.

The TGA has commenced consultation, through CSIRO Futures, in the areas of Software as a Medical Device (SaMD), and Cyber Security for Medical Devices (CSfMD). Regulation of SaMD is challenged by the emergence of new players that may not have had the opportunity to engage with the TGA, or are lacking an awareness of the regulatory requirements in Australia. CSfMD challenges arise due to the increasing impact and complexity of the cyber threat landscape, and the lack of current regulatory guidelines to effectively address this.

https://www.tga.gov.au/research-software-medical-device-and-cyber-security-medical-devices
Watch their first workshop here: https://research.csiro.au/tga/cyber-security-for-medical-devices-guidelines/

NOVA LEAH
SELECTEVIDENCE



Consistent Themes Across the Globe

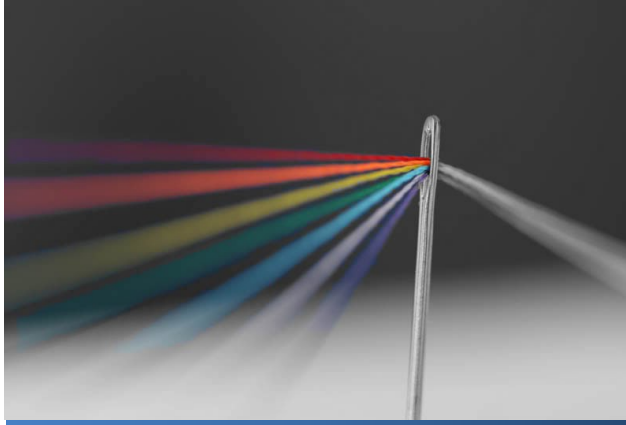
- Security Risk Management
  - Starts with understanding and controlling risk. Foundational to everything.
- Security-by-Design
  - Designing technical controls to ensure comprehensive and robust protection
- Standards
  - Utilization of appropriate standards
- Documentation
  - Demonstrating assurance that manufacturers are doing the right things

Finding the Common Thread

Identifying Themes across the Globe

Standards Update

NOVA LEAH
SELECTEV/DENCE



Standards in Development

ISO/IEC

ISO 81001-1 Health software and health IT systems safety, effectiveness and security -- Part 1: Foundational principles, concepts, and terms

(New Proposal**) 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

(Revision) **IEC 62304** Medical device software -- Software life cycle processes

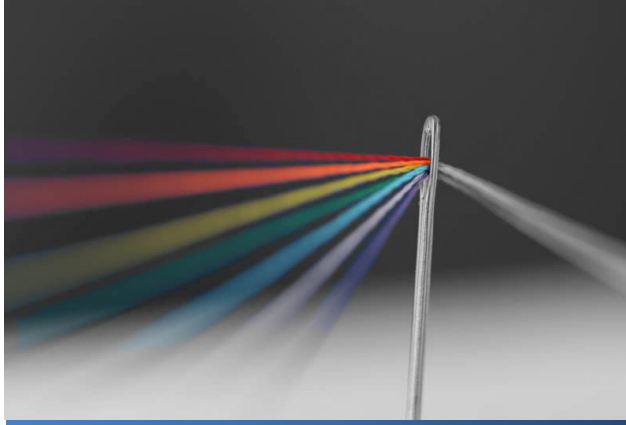
AAMI

AAMI TIR97/Ed.1, Principles for medical device security – Post-market security management for device manufacturers

AAMI SW96/Ed.1, Medical Devices - Application of security risk management to medical devices

Keeping an Eye on the Future

NOVA LEAH
SELECTEVIDENCE

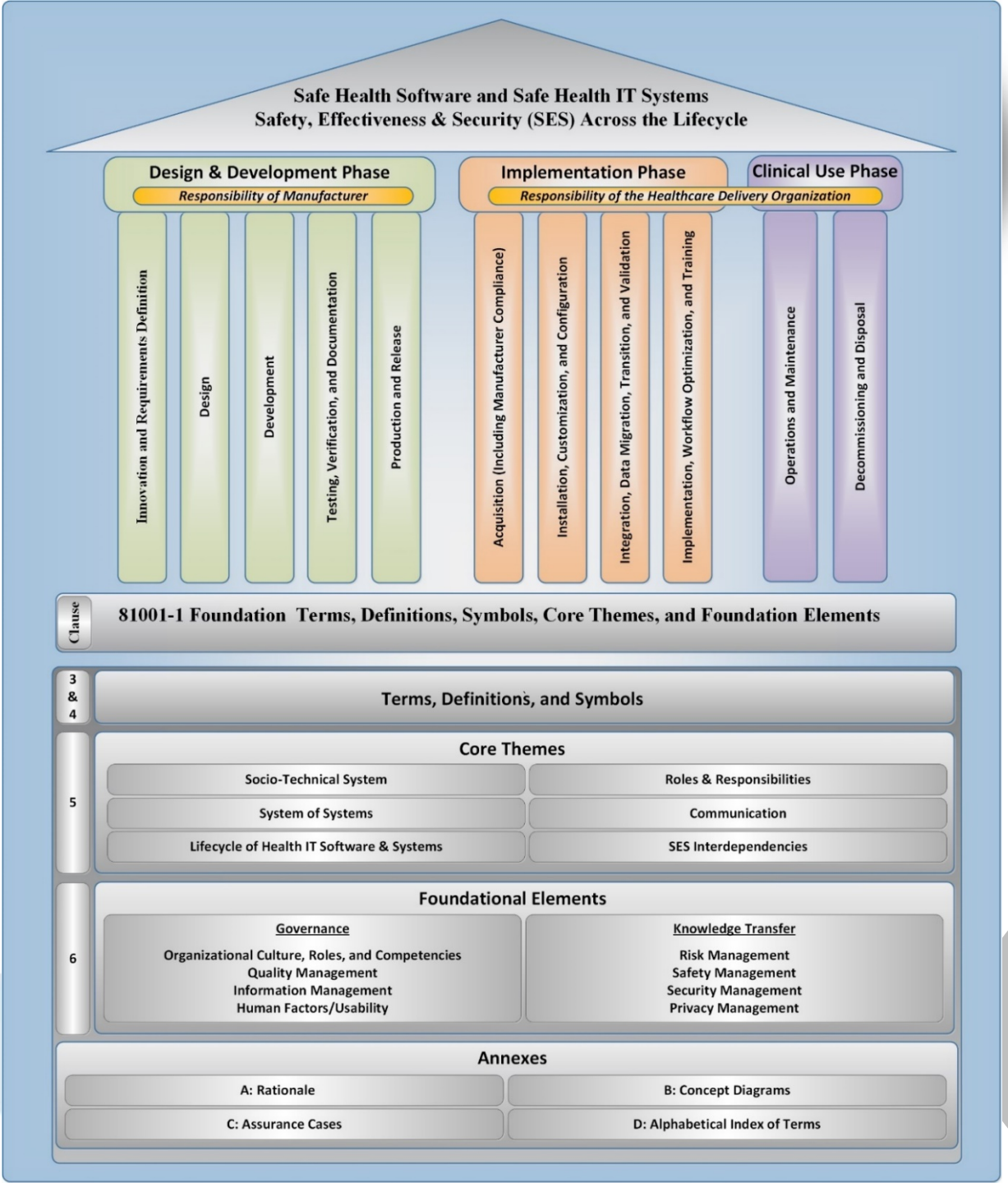


ISO/IEC 81001

- Title: Health software and health IT systems safety, effectiveness and security - Foundational principles, concepts and terms
- Scope
  - Articulates foundational principles, concepts, and terms for health software and health IT system safety across the full life cycle from concept to decommission
- Approach
  - Identify and align common terminology
  - Highlight foundational elements and core themes
- Next Steps: CD2 out for comment

ISO TC 215
JWG 7

Developing Standards



ISO TC 215 JWG 7

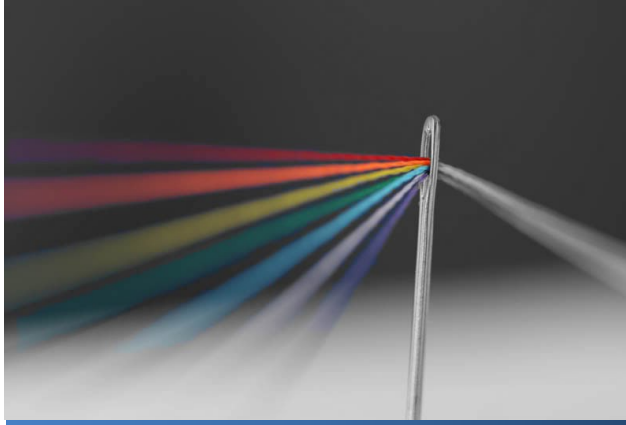
Developing Standards

NOVA LEAH

SELECTEV/DENCE

Clause	81001-1 Foundation Terms, Definitions, Symbols, Core Themes, and Foundation Elements
3 & 4	Terms, Definitions, and Symbols
5	**Core Themes** Socio-Technical System Roles & Responsibilities System of Systems Communication Lifecycle of Health IT Software & Systems SES Interdependencies
6	**Foundational Elements** Governance Organizational Culture, Roles, and Competencies Quality Management Information Management Human Factors/Usability Knowledge Transfer Risk Management Safety Management Security Management Privacy Management
	Annexes A: Rationale B: Concept Diagrams C: Assurance Cases D: Alphabetical Index of Terms

NOVA LEAH
SELECTEVIDENCE



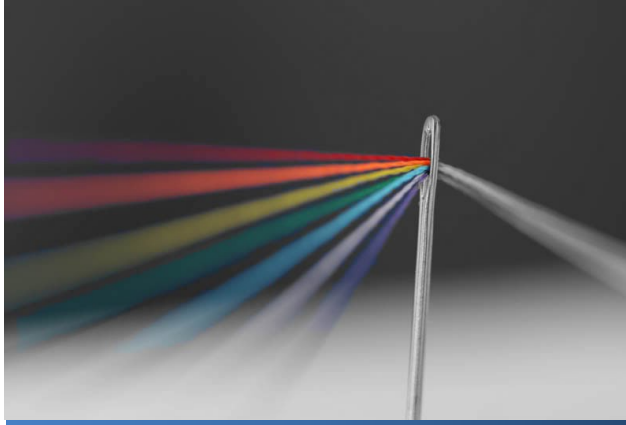
IEC 80001-5-1

- Title: Application of risk management for IT-networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 5-1: Activities in the product lifecycle
  - (Title currently missing the security-specific nature of the document)
- Scope
  - Specifies activities in the product lifecycle of health software toward the (information) security of the product
- Approach
  - Plan to structure around IEC 62304 but will address activities specific to security
- Next Steps: Kick-off in Germany Feb 4-6, 2019

ISO TC 215
JWG 7

Developing Standards

NOVA LEAH
SELECTEVIDENCE



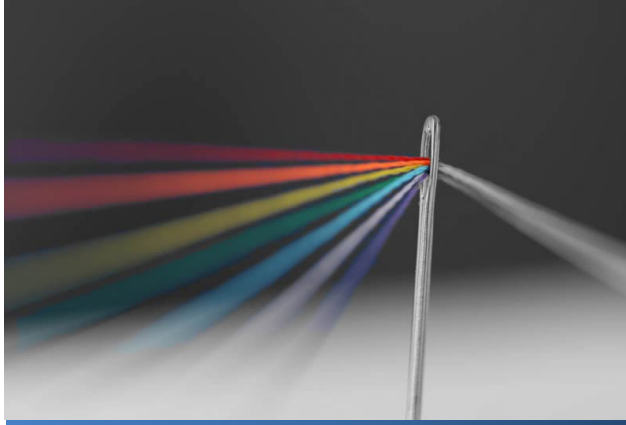
IEC 62304 Revision

- Title: Medical device software - - Software life cycle processes
- Status
  - Recently voted down. TG currently working to resolve
- Issue in Discussion
  - Main issue is whether to require ISO 14971

ISO TC 215
JWG 7

Developing Standards

NOVA LEAH
SELECTEVIDENCE



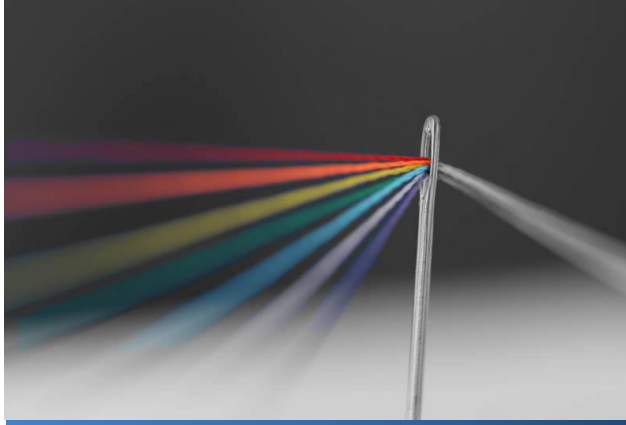
AAMI TIR 97

- Title: Principles for medical device security — Postmarket risk management for device manufacturers
- Status
  - Recently resolved CDV-2 comments

AAMI

Developing Standards

NOVA LEAH
SELECTEVIDENCE



AAMI TIR 97 Topics

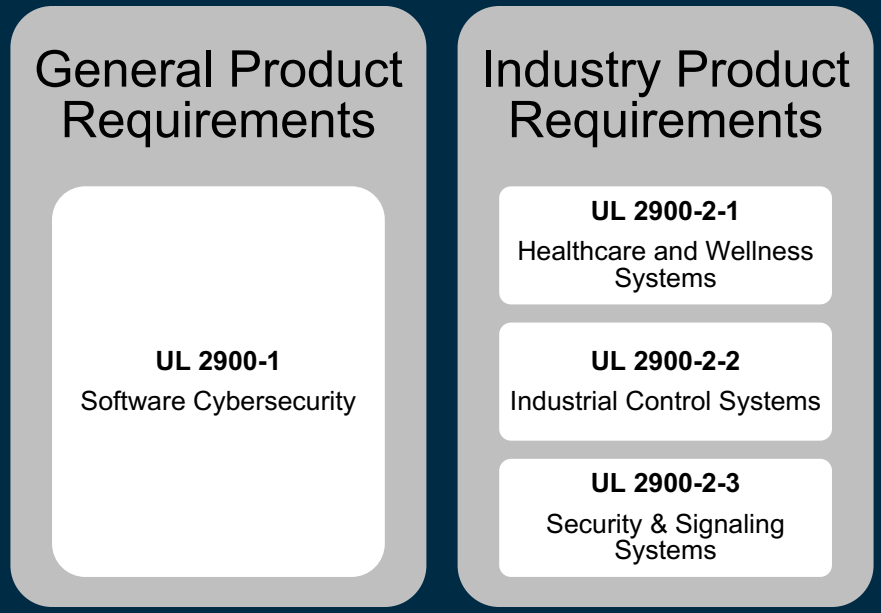
1. Postmarket considerations for security policies and security program administration
2. Design features for postmarket security risk management
3. Installation and configuration
4. Postmarket management of fielded devices
5. Retirement/obsolescence
6. Annex A: Sample medical device security policy statements
7. Annex B: Security risk management for healthcare networks
8. Annex C: Establishing a coordinated vulnerability disclosure process
9. Mapping of defined terms from FDA postmarket guidance

AAMI

Developing Standards

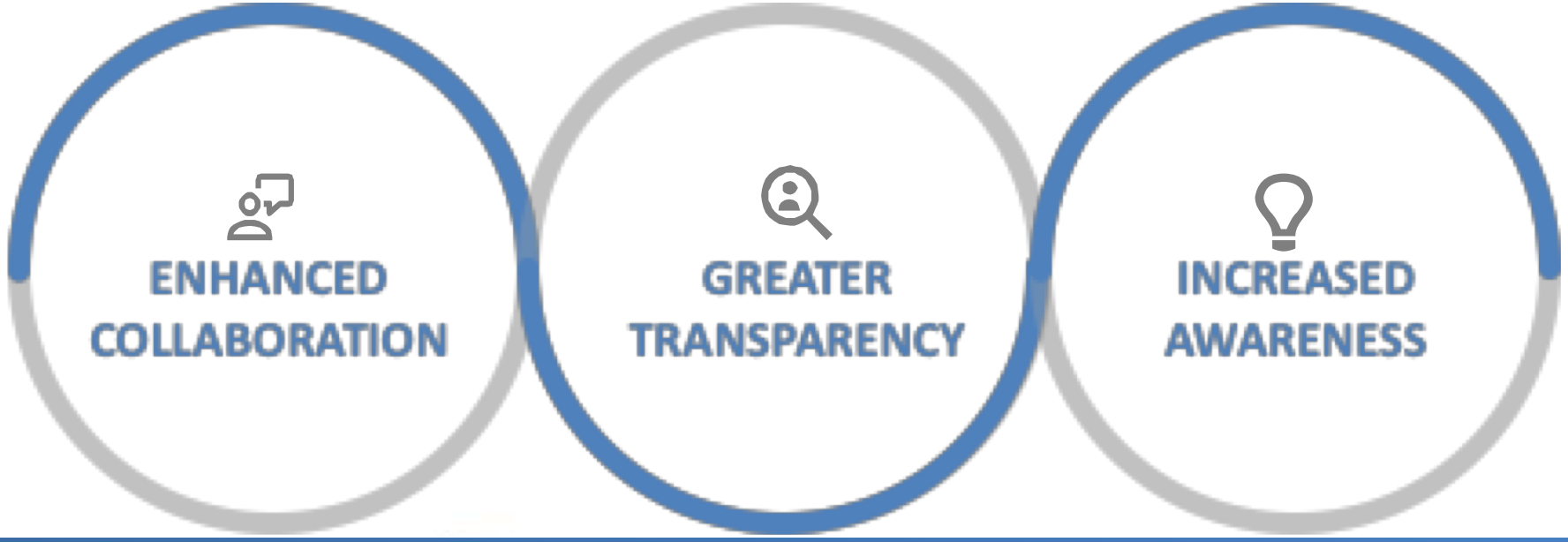
UL 2900 Series of Standards

- Offer transparent & testable cybersecurity criteria that can be used across industry verticals to repeatably and reproducibly measure the security posture of products and address the basic cyber-hygiene of products
- Technical criteria in UL 2900 are based on existing industry best practices and guidance documents
- UL 2900-1 / 2900-2-1 standards are ANSI / SCC approved binational standards
- UL 2900-1 / 2900-2-1 are US FDA Recognized Consensus Standards



NOVA LEAH
SELECTEV/DENCE

THE SECURITY OF MEDICAL DEVICE WILL DEPEND ON...



INDUSTRY EXPECTATIONS

SELECTEVIDENCE

Thank you

Michelle Jump
michelle.jump@novaleah.com