IOT101

Biggest Security Trends and What to Expect

Michael Dow
Senior Manager – Secure Wireless Technology Product Management
SILICON LABS

Agenda

01 The World-Wide Security Regulatory Landscape

02 World-Wide Certification?

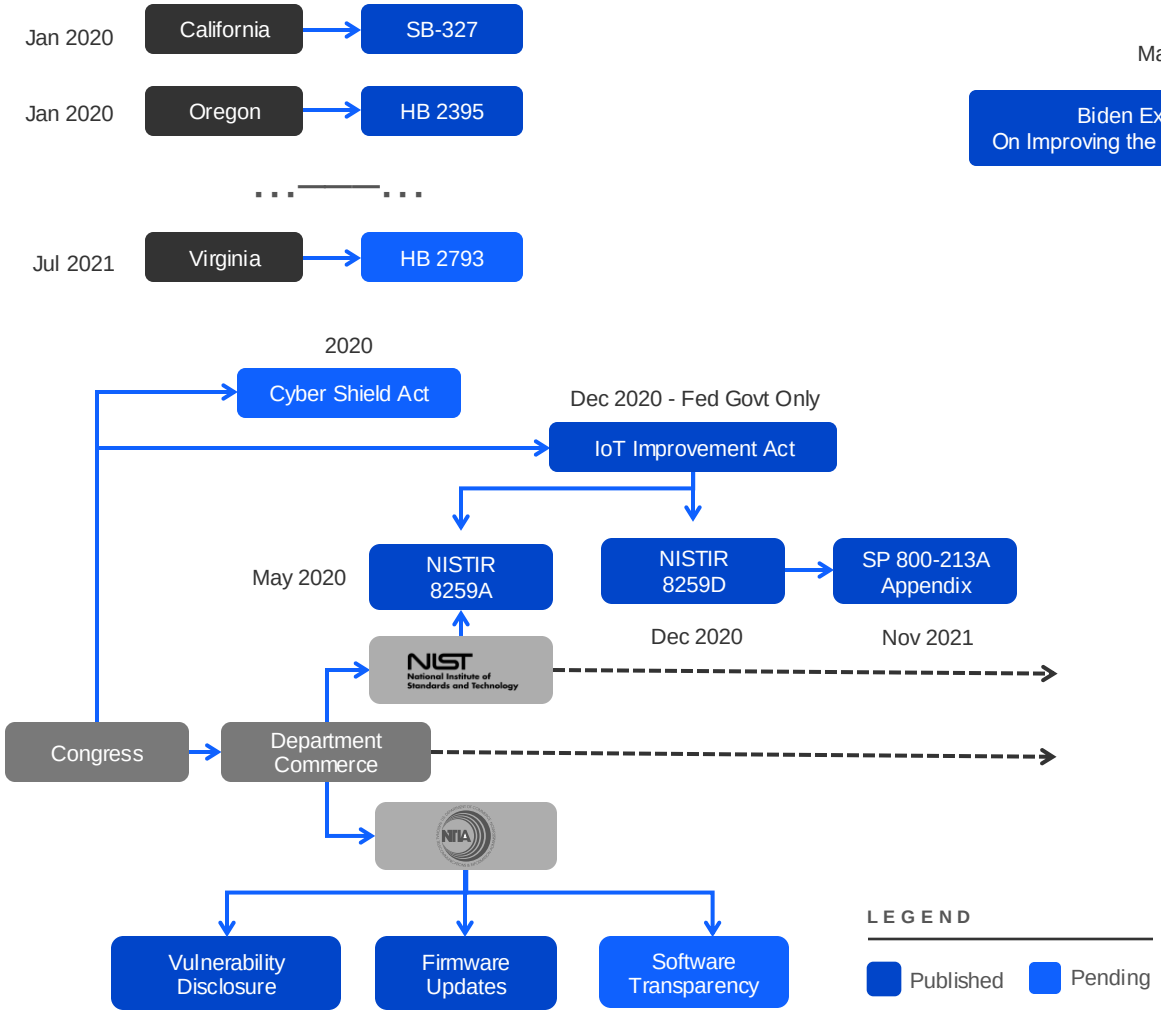
03 Secure By Design

04 Software Bill of Materials (SBOM)

05 Q&A

World-Wide Security Regulatory Landscape

Governmental Regulatory Landscape — United States



May 2021 — Biden Executive Order On Improving the Nation's Cybersecurity

Jun 2022 — NIST IR 8425 ipd

July 2023 — US IoT Security Labeling Program

Profile of the IoT Core Baseline for Consumer IoT Products

Requirement	Federal Requirement
Asset Identification **(Secure Identity)**	The IoT product is uniquely identifiable and inventories all of the IoT product's components
Product Configuration **(Secure Boot)**	The IoT product configuration is changeable, ability to restore a secure default setting, changes only performed by authorized entities
Data Protection **(Cryptography)**	The IoT product can protect the data it stores and transmits from unauthorized access, disclosure, and modification.
Interface Access Control **(Secure Debug)**	The IoT product restricts access to all interfaces to limit access to only authorized entities
Software Update **(Secure OTA Updates)**	The IoT product's software can be updated by authorized entities only by using a secure and configurable mechanism.
Cybersecurity State Awareness **(Tamper)**	The IoT product supports detection of cybersecurity incidents affecting or affected by the IoT product and they store and transmit

May 2021 - President Biden Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the

(t) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

June 2022 - NIST IR 8425 – Consumer IoT Product Security Profile

NIST IR 8425 ipd

Profile of the IoT Core Baseline for Consumer IoT Products

Initial Public Draft

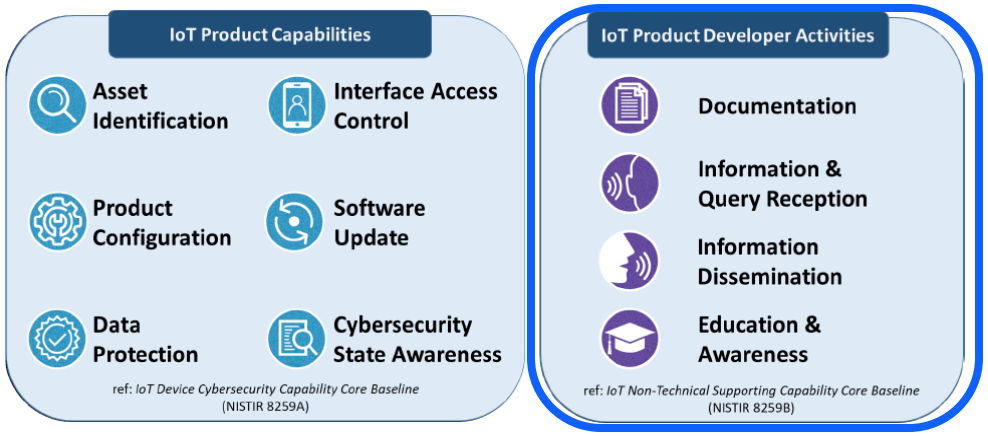
Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425.ipd

June 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology



2.2.1 IoT Product Capabilities

Asset Identification

The IoT product is uniquely identifiable and inventories all of the IoT product's components.

1. The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).
2. The IoT product uniquely identifies each IoT product component and maintains an up-to- date inventory of connected product components.

Cybersecurity utility: The ability to identify IoT products and their components is necessary to support asset management for updates, data protection, and digital forensics capabilities for incident response.

July 2023 – Biden Administration Announces Cybersecurity Labeling Program

Administration Prio

JULY 18, 2023

Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers

BRIEFING ROOM ▸ STATEMENTS AND RELEASES

Leading electronics and appliance manufacturers and retailers make voluntary commitments to increase cybersecurity on smart devices, help consumers choose products that are less vulnerable to cyberattacks.

March 2024 - Cyber Trust Mark – FCC Launches Cyber Trust Labeling Program

U.S. CYBER TRUST MARK

FCC NEWS from the Federal Communications Commission

Media Contact:
Office of Media Relations
MediaRelations@fcc.gov

For Immediate Release

FCC CREATES VOLUNTARY CYBERSECURITY LABELING PROGRAM FOR SMART PRODUCTS

'U.S. Cyber Trust Mark' Program Will Help Consumers Make Informed Purchasing Decisions and Encourage Manufacturers to Meet Higher Cybersecurity Standards

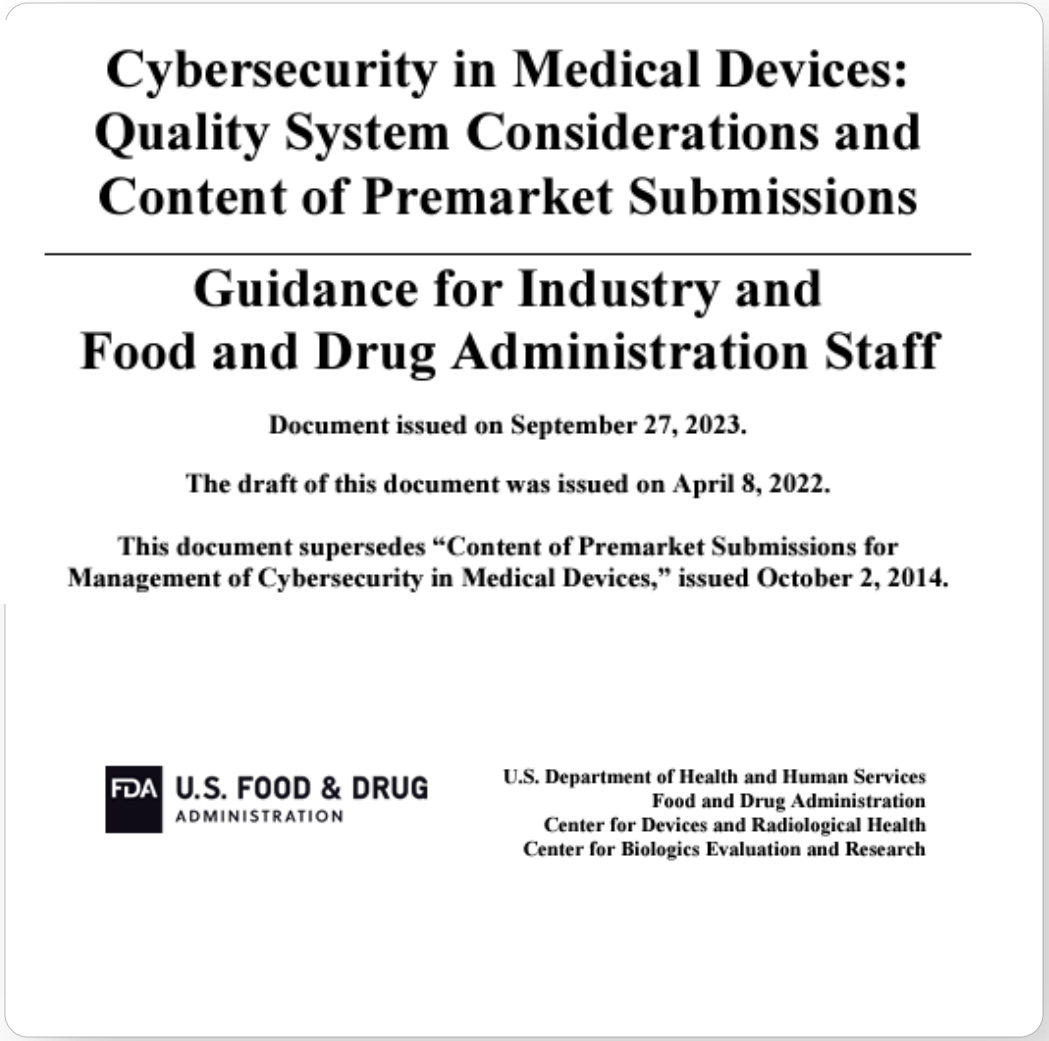
WASHINGTON, March 14, 2024— The Federal Communications Commission today voted to create a voluntary cybersecurity labeling program for wireless consumer Internet of Things ("IoT") products. Under the program, qualifying consumer smart products that meet robust cybersecurity standards will bear a label—including a new "U.S Cyber Trust Mark"—that will help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards.

February 22, 2024

FCC FACT SHEET*
Cybersecurity Labeling for Internet of Things
Report and Order PS Docket No. 23-239

- Products w/ radios only
- NIST IR 8425 as Basis
- Product includes end node, mobile app, and cloud sftw

Sept 27, 2023 – FDA - Cybersecurity in Medical Devices Guidance



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

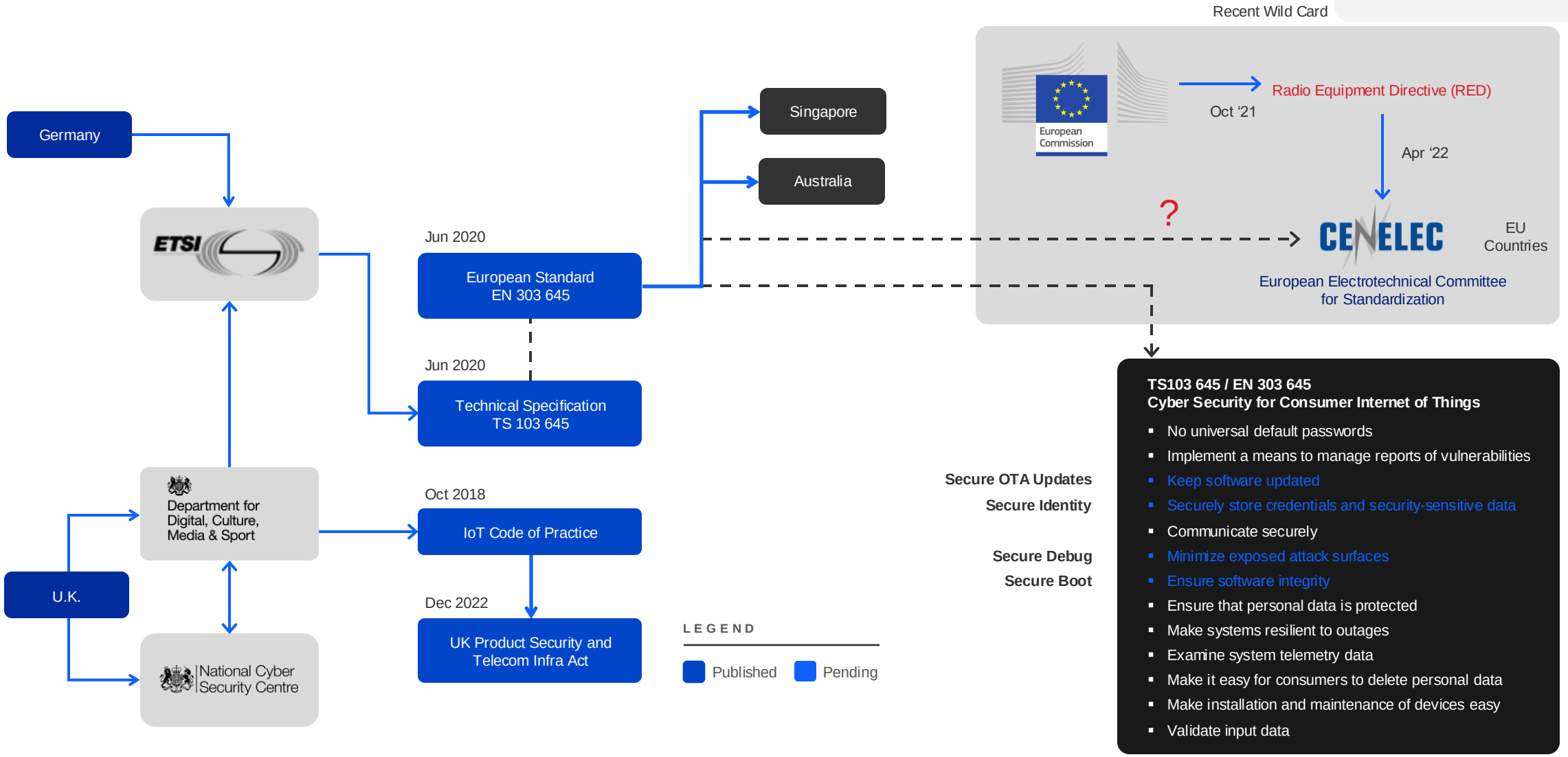
This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

- Secure Product Development Framework (SPDF)
  - Threat Modeling
  - Risk due to standard communication protocols such as BLE/WiFi
  - Third party software vulnerabilities
  - SBOMs linked to Common Vulnerabilities and Exposures (CVE) Databases
  - Manufactures should ensure appropriate resources to identify, assess, and mitigate security vulnerabilities through the Total Product Life Cycle (TPLC)
  - Cyber Security Transparency
    - Labeling Recommendations
    - Cybersecurity Management Plans
  - Security Architecture w/ Security Controls (very detailed)
    - Authentication of Information and Entities
    - Authorization – Principle of least privileges
    - Cryptography – current NIST Standards
    - Code, Data, and Execution Integrity
    - Confidentiality
    - Event Detection and Logging
    - Resiliency and Recovery
    - Firmware and Software Updates

Governmental Regulatory Landscape – Europe



Dec 2022- UK – Product Security and Telecom Infra Act 2022

First EU Regulation in Force in May 2024

THE ACT

- **Scope – Connectable products made available to consumers in the UK**
- **Connectable Products –**
  - Internet-Connectable - Directly connected to the internet via an internet protocol suite **OR**…
  - Network-Connectable – product is connectible to two or more products at the same time via a non-IP protocol **AND** can connect directly to an Internet-Connectable product
- **Excludes the following products as they are regulated by separate legislation: Smart Meters, Smart Charge Points, Medical Devices**

END PRODUCT REQUIREMENTS – NOT COMPONENT

- **Unique Passwords per product**
- **Public mechanism for reporting vulnerabilities**
- **IF the product is capable of receiving security updates - Defined support period for providing security updates free of charge (Security Warranty)**

2 DOCUMENTS – THE ACT – THE REQUIREMENTS

Product Security and Telecommunications Infrastructure Act 2022

STATUTORY INSTRUMENTS

2023 No. 1007

CONSUMER PROTECTION

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023

European Union - Radio Equipment Directive (RED) Security Requirements

2014 DIRECTIVE 53 – ARTICLE 3(3)

(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service; *(example given: Denial of Service)*

(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

(f) radio equipment supports certain features ensuring protection from fraud;

OCT 29, 2021 – SUPPLEMENT TO 2014 DIRECTIVE 53

- Deadline set for August 1st, 2024 – first regulation to specify compliance date
- Compliance date depends on "Voluntary Harmonized Standards" being in place and industry adopted – i.e.CENELEC -> ETSI EN 303 645?
- Any device must be "capable itself to communicate over the internet" *(IPv(X) based comms i.e. WiFi or Thread)*
  - Exception: childcare, toys, and wearables are in scope even if connected to a gateway *(i.e. ZigBee, Z-Wave, Proprietary)*

Radio Equipment Directive (RED)

Applies To:

- **Devices capable of communicating via the Internet:** Examples of such equipment include electronic devices such as smartphones, tablets, electronic cameras; telecommunication equipment as well as equipment that constitutes the 'internet of things'.
- **Toys and childcare equipment:** Toys and baby monitors can be vulnerable to cybersecurity threats that monitor or collect information about children.
- **Wearables:** Devices like smartwatches and fitness trackers.

RED - CENELEC Joint Technical Committee (JTC) 13 / Work Group (WG) 8 - Likely in effect in 2025

3 DOCUMENTS CURRENTLY BEING WORKED

Doc #	Radio Equipment Catagory
1	Internet connected radio equipment
2	Radio equipment that processes Personal, Traffic, or Location Data that is internet connected OR designed or intended for Childcare, Toys, or Wearables (even if non-internet connected)
3	Internet connected radio equipment that enables user to transfer, monetary value, or virtual currency

STANDARDIZATION REQUEST (SCOPE)

"… shall contain technical specifications that ensure… radio equipment, where applicable:

- Monitor and control network traffic
- Mitigate DOS attacks
- Up-to-date software without known vulnerabilities
- Secure mechanisms for updating software and firmware
- Protect exposed attack surfaces and minimize impact of attacks
- Protect personal and financial data at rest and during transit
- Inform users of changes that affect data protection and privacy
- Log internal activity that may affect security of the above
- Allow users to easily delete personal data

CURRENT DRAFT REQUIREMENTS AS OF MARCH 2024

Doc #	Security Function	Purpose
All	Access control mechanism	access control of resources
All	Authentication mechanism	the entity is what it claims to be
All	Secure Update mechanism	patch vulnerabilities
All	Secure storage mechanism	privileged data at rest
All	Secure communication mechanism	privileged data in motion
All	Confidential Cryptographic Keys	guidance on key size, use, and storage
All	General equipment capabilities	up-to-date software and hardware with no known "exploitable" vulnerabilities, no unnecessary external interfaces
All	Cryptography	shall use for Secure Update, Secure Storage, Secure Comms, CSP generation, etc.
1	Resilience mechanism	mitigate DOS attack and return to defined state after attack
1	Network monitoring mechanism	detect DOS and defend
1	Traffic control mechanism	source address validation
2	User notification mechanism	notify user of changes of privileged data
2	Deletion mechanism	deletion of privileged data
2,3	Logging mechanism	events that might impact privileged data

Cyber Resiliency Act (CRA) – Competes with RED - Likely in effect in 2025

SECURITY FUNCTIONS

- Designed, developed, and produced with appropriate level of security based on risk
- Delivered without any known vulnerabilities
- Based on Risk Assessment:
  - Secure by default
  - Protection from unauthorized access
  - Confidentiality and Integrity of data at rest and in motion
  - Security updates
  - Secured interfaces
  - Secured against of DOS attacks

PRODUCT PROCESS REQUIREMENTS

- Public security support policy and period of service (Security Warranty)
- Publicly available SBOM in machine-readable format
- Publicly identify, document, and remediate vulnerabilities free of charge
- Regular security reviews and testing
- Publicly available documentation on security use, how to apply security updates, and how to securely decommission the device

CYBER SECURITY REQUIREMENTS - ANNEXES 1-6

Brussels, 15.9.2022
COM(2022) 454

ANNEXES 1 to 6

ANNEXES

to the

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

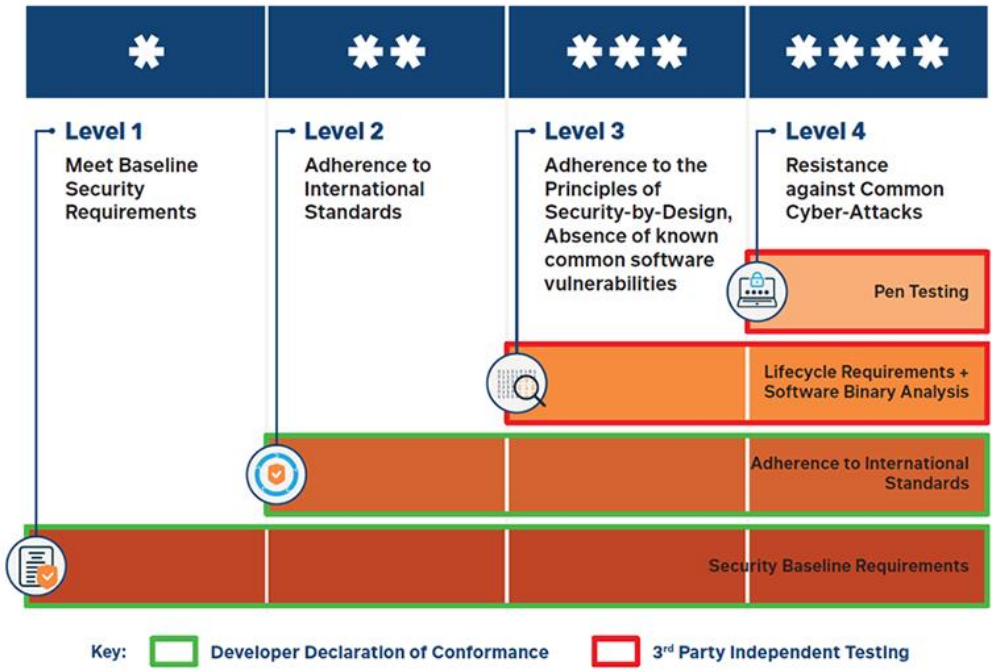
{SEC(2022) 321} - {SWD(2022) 282} - {SWD(2022) 283}

Singapore Cybersecurity Labeling Scheme (CSL)

Voluntary for now but will likely become mandatory

MARCH 2020

Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE



Level 1 (Self Assessment)

- No Universal Passwords
- Report Vulnerabilities
- Keep Software Securely Updated

Level 2 (Self Assessment)

- Meet all selected ETSI 303 645 Requirements

Level 3 (Level 2 + Lab Verification)

- Secure By Design
  - Threat Modeling
  - Secure by Design (Software/Hardware)
  - Secure Supply Chain w/ no known vulnerabilities
  - Publish Security Policies
  - Penetration Testing and Hardening
- Software contains no known vulnerabilities

Level 4 (Level 3 + Black Box Pen Testing

- Perform prescribed minimum test
  - Ports and Services
  - Firmware and Software Updates
  - Communications
  - Configuration Portal
  - Mobil Applications
  - Authentication
  - Physical Attacks
  - Simple Side Channel Analysis & Fault Injection
  - Interfaces: JTAG, UART, Debug, etc
- 4 Days of Freedom Pen Testing
- Automated Fuzz Testing

May 2023 - India IoT Standards from the Bureau of Indian Standards

Released May 18, 2023 — Voluntary for now

NIST IR 8228

ETSI EN 303 645

OWASP

Functions

Organization of cybersecurity activities at highest level

Functions	Description	# of Requirements
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	42
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.	143
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	304
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	10
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident	26

Total: 525

Assurance Levels

Assurance levels are defined in this part of the standard, and their suitability is subject to change with application specific concerns (e.g., intended usage, connectivity to valuable applications/networks, user security requirements, value of assets, functions and deployment scenarios).

Level 0	where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organisation.
Level 1	where compromise to the data generated or loss of control is likely to result in limited impact on an individual or organisation
Level 2	The device is designed to resist attacks on availability that would have significant impact on an individual or organisation, or impact many individuals, for example by limiting operations of an infrastructure to which it is connected.

Bureau of Indian Standards
The National Standards Body of India

Sl. No.	Function	Requirements	Assurance Level		
			L0	L1	L2
Control-01					
SR8.	Identify	A transparent and auditable policy shall be in place to update software/firmware of IoT components to fix any known vulnerability and notify respective users.	✗	✓	✓
SR21.	Identify	The mapping of cryptographic identities with chip identifiers shall be defined and backed up with IoT service provider.	✗	✓	✓
SR66.	Protect	Only necessary communication interfaces, network protocols, application protocols and network services shall be enabled.	✗	✓	✓
SR74.	Protect	The random number generator shall be used for all relevant cryptographic operations e.g. generation of nonce, initialization vectors and keys.	✗	✓	✓
SR78.	Protect	The secure boot loader shall be stored in a secure environment of executable memory, where it shall be read, but not altered (e.g. internal ROM/lock-capable NVRAM/One Time Programmable Memory etc.).	✗	✓	✓
SR84.	Protect	The secure boot process shall be enabled by default and shall not be configurable.	✓	✓	✓
SR85.	Protect	The IoT product shall have an irrevocable Hardware Secure Boot process.	✓	✓	✓
SR92.	Protect	The rogue or compromised applications shall be prevented from accessing areas of memory containing privileged resources such as TEE, trust anchor driver, hardware peripheral registers or cryptographic parameters using memory protection techniques (e.g. Security Memory Protection Unit).	✗	✓	✓
SR108.	Protect	All keys shall be stored securely in accordance with Industry best practices (e.g. FIPS 140-2 or FIPS 140-3 or ISO/IEC 19790:2012).	✗	✓	✓

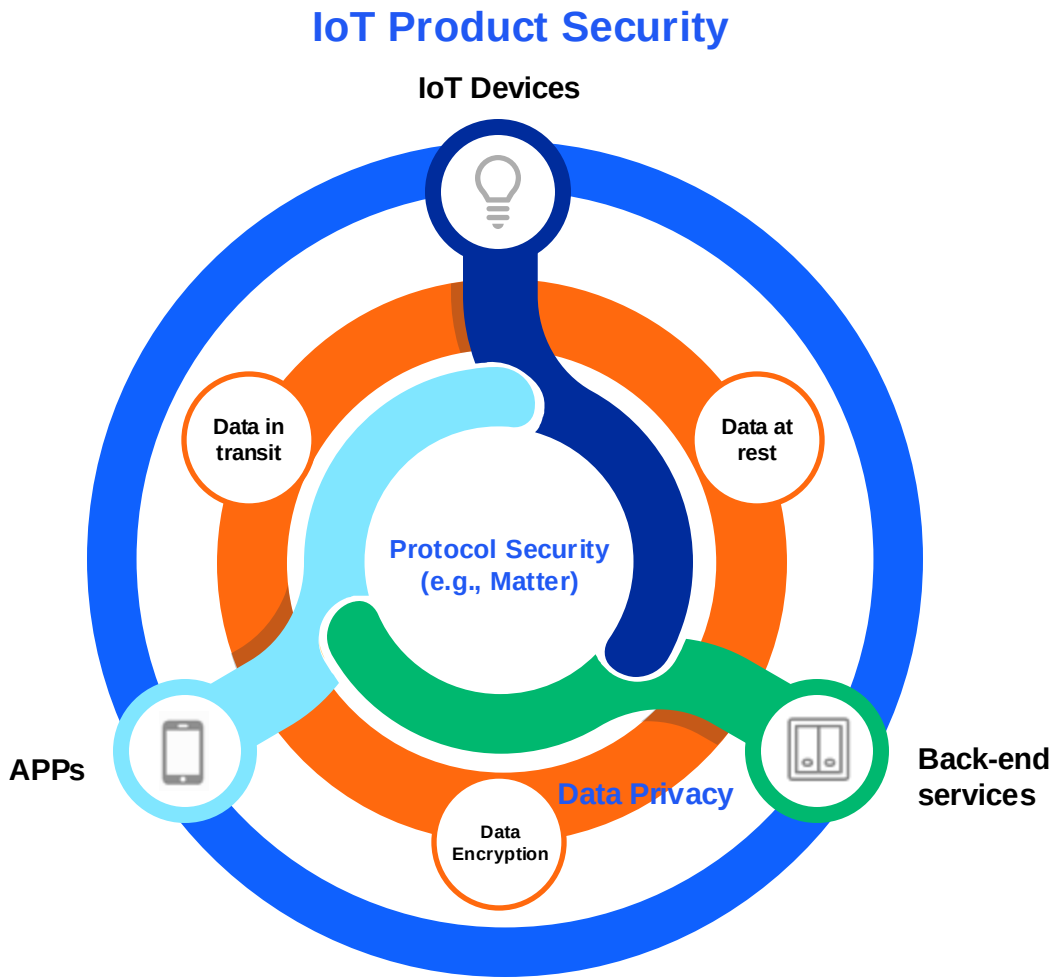
World-Wide Certification?

EXAMPLE

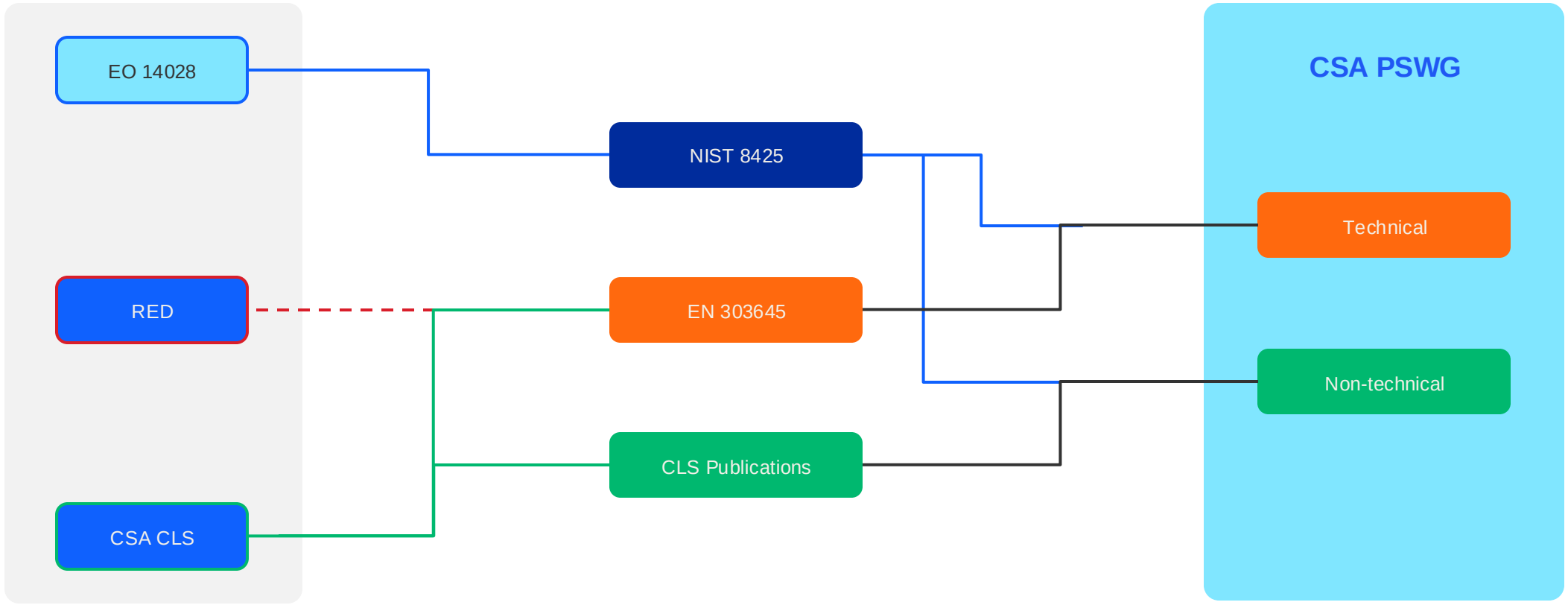
Connectivity Standards Alliance (CSA) Product Security Certification

Protocol Security vs. Data Privacy vs. Product Security

Verified
PRODUCT SECURITY
by Connectivity Standards Alliance™



First Tech Spec and Certification Program Approved – v1.0 – April 2024



PSWG Certification

Conformance Evidence:

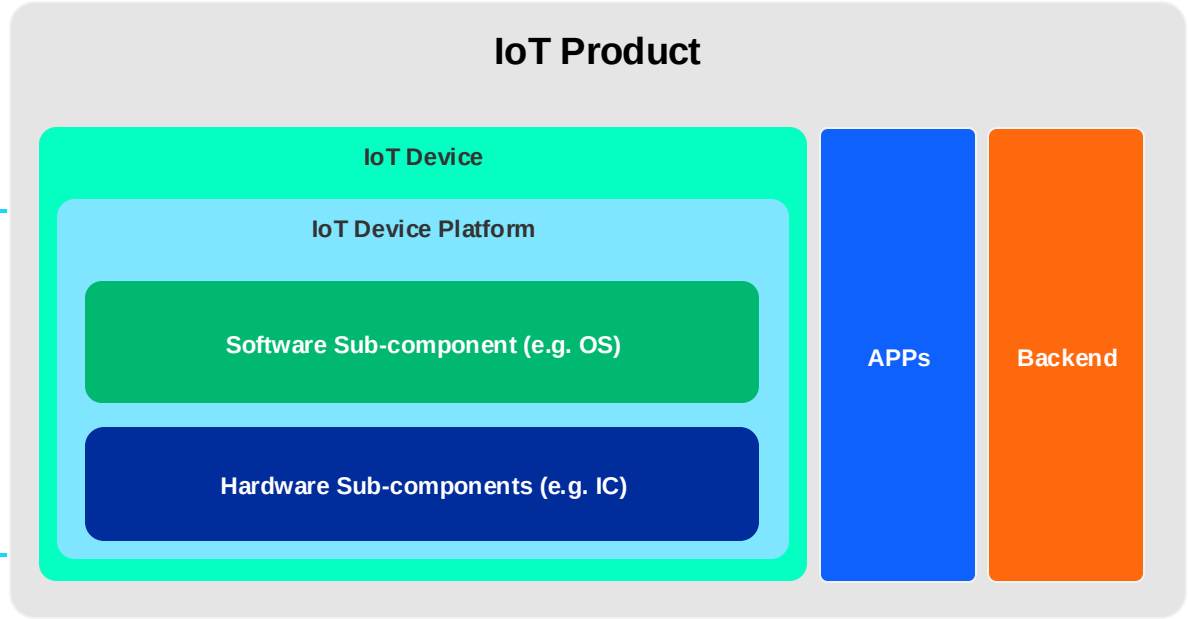
- EU RED
- USA IoT Labelling
- Singapore CSA CLS
- …

CSA PSWG

IoT Device Certification

CSA PSWG Dependent Certification Programs

CC, SESIP, PSA Certified



Secure By Design

June 2022 - NIST IR 8425

Requires elements of SDLC

NIST IR 8425 ipd

Profile of the IoT Core Baseline for Consumer IoT Products

Initial Public Draft

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425.ipd

June 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

2.2.2 IoT Product Non-Technical Supporting Capabilities

Documentation

v. Secure software development and supply chain practices used.
vi. Accreditation, certification, and/or evaluation results for cybersecurity – related practices.

i. Steps taken during development to ensure the IoT product and its product components are free of any known, exploitable vulnerabilities.

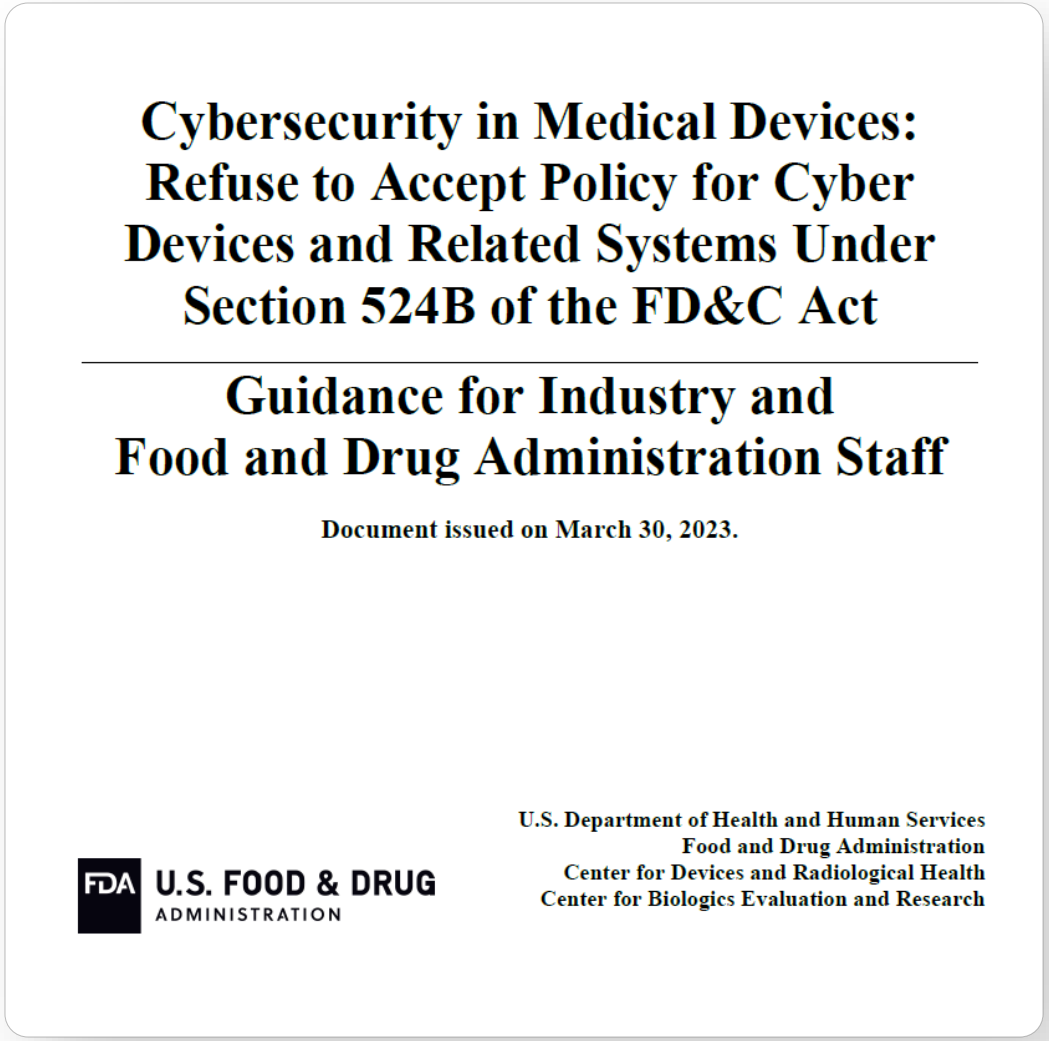
Information and Query Reception

The ability of the IoT product developer to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.

1. The IoT product developer can receive information related to the cybersecurity of the IoT product and its product components and can respond to queries related to cybersecurity of the IoT product and its product components from customers and others, **including**:
   a. The ability of the IoT product developer to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from customers and others in the IoT product ecosystem (e.g., repair technician acting on behalf of the customer).
   b. The ability of the IoT product developer to receive queries from and respond to customers and others in the IoT product ecosystem about the cybersecurity of the IoT product and its components.

March 30, 2023 - US Food and Drug (FDA)

Cybersecurity in Medical Devices will require SDLC



Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act

Guidance for Industry and Food and Drug Administration Staff

Document issued on March 30, 2023.

U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

II.Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-

(2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address—

(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

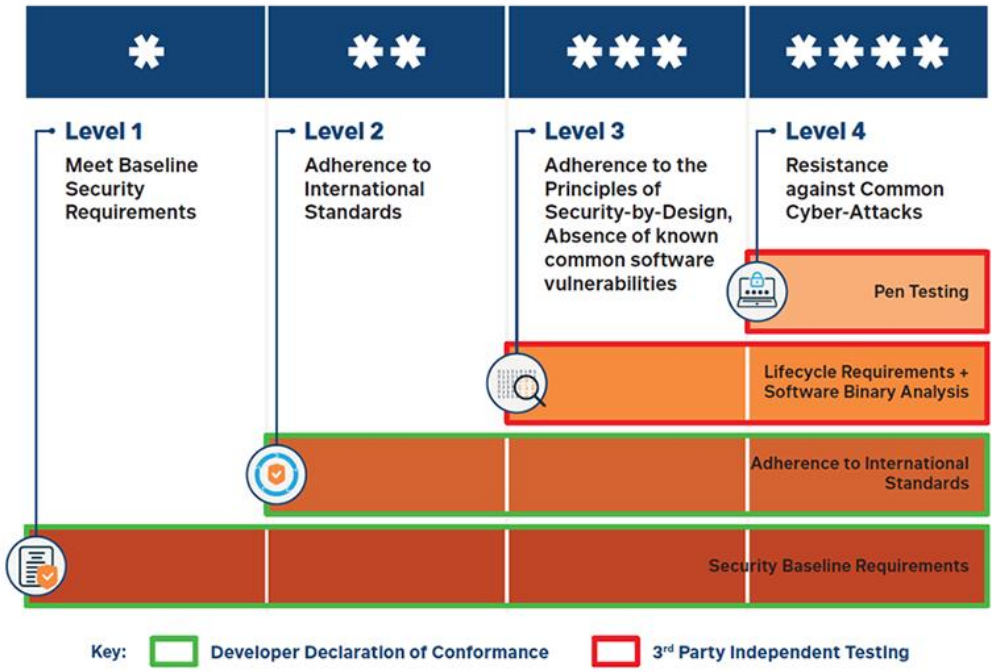
(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

Singapore Cybersecurity Labeling Scheme (CSL)

Voluntary for now but will likely become mandatory

MARCH 2020

Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE



Level 1 (Self Assessment)

- No Universal Passwords
- Report Vulnerabilities
- Keep Software Securely Updated

Level 2 (Self Assessment)

- Meet all selected ETSI 303 645 Requirements

Level 3 (Level 2 + Lab Verification)

- Secure By Design
  - Threat Modeling
  - Secure by Design (Software/Hardware)
  - Secure Supply Chain w/ no known vulnerabilities
  - Publish Security Policies
  - Penetration Testing and Hardening
- Software contains no known vulnerabilities

Level 4 (Level 3 + Black Box Pen Testing

  - Perform prescribed minimum test
  - Ports and Services
  - Firmware and Firmware Updates
  - Communications
  - Configuration Portal
  - Mobil Applications
  - Authentication
  - Physical Attacks
  - Simple Side Channel Analysis & Fault Injection
  - Interfaces: JTAG, UART, Debug, etc
- 4 Days of Freedom Pen Testing
- Automated Fuzz Testing

Cyber Resiliency Act (CRA) – Competes with RED - Likely in effect in 2025

SECURITY FUNCTIONS

- Designed, developed, and produced with appropriate level of security based on risk
- Delivered without any known vulnerabilities
- Based on Risk Assessment:
  - Secure by default
  - Protection from unauthorized access
  - Confidentiality and Integrity of data at rest and in motion
  - Security updates
  - Secured interfaces
  - Secured against of DOS attacks

PRODUCT PROCESS REQUIREMENTS

- Public security support policy and period of service (Security Warranty)
- Publicly available SBOM in machine-readable format
- Publicly identify, document, and remediate vulnerabilities free of charge
- Regular security reviews and testing
- Publicly available documentation on security use, how to apply security updates, and how to securely decommission the device

CYBER SECURITY REQUIREMENTS - ANNEXES 1-6

EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454

ANNEXES 1 to 6

ANNEXES

to the

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

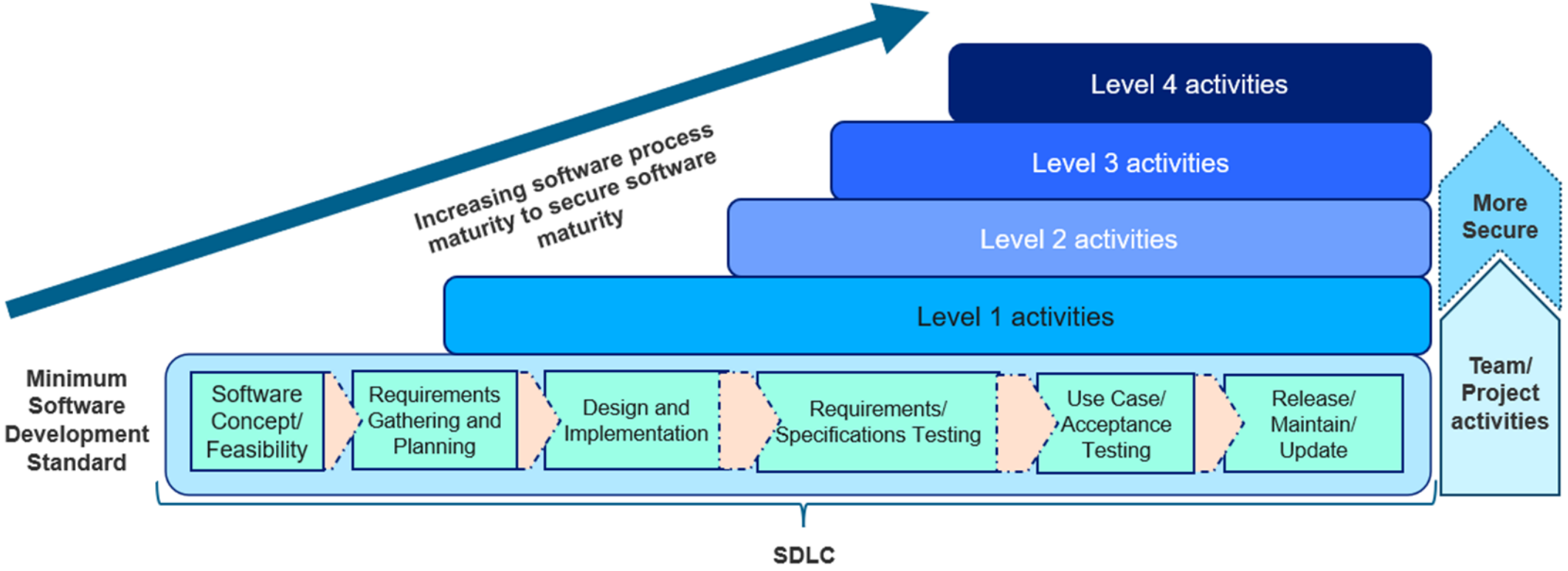
{SEC(2022) 321} - {SWD(2022) 282} - {SWD(2022) 283}

The new Total Product Development Lifecycle (TPDL) – DevSecOps

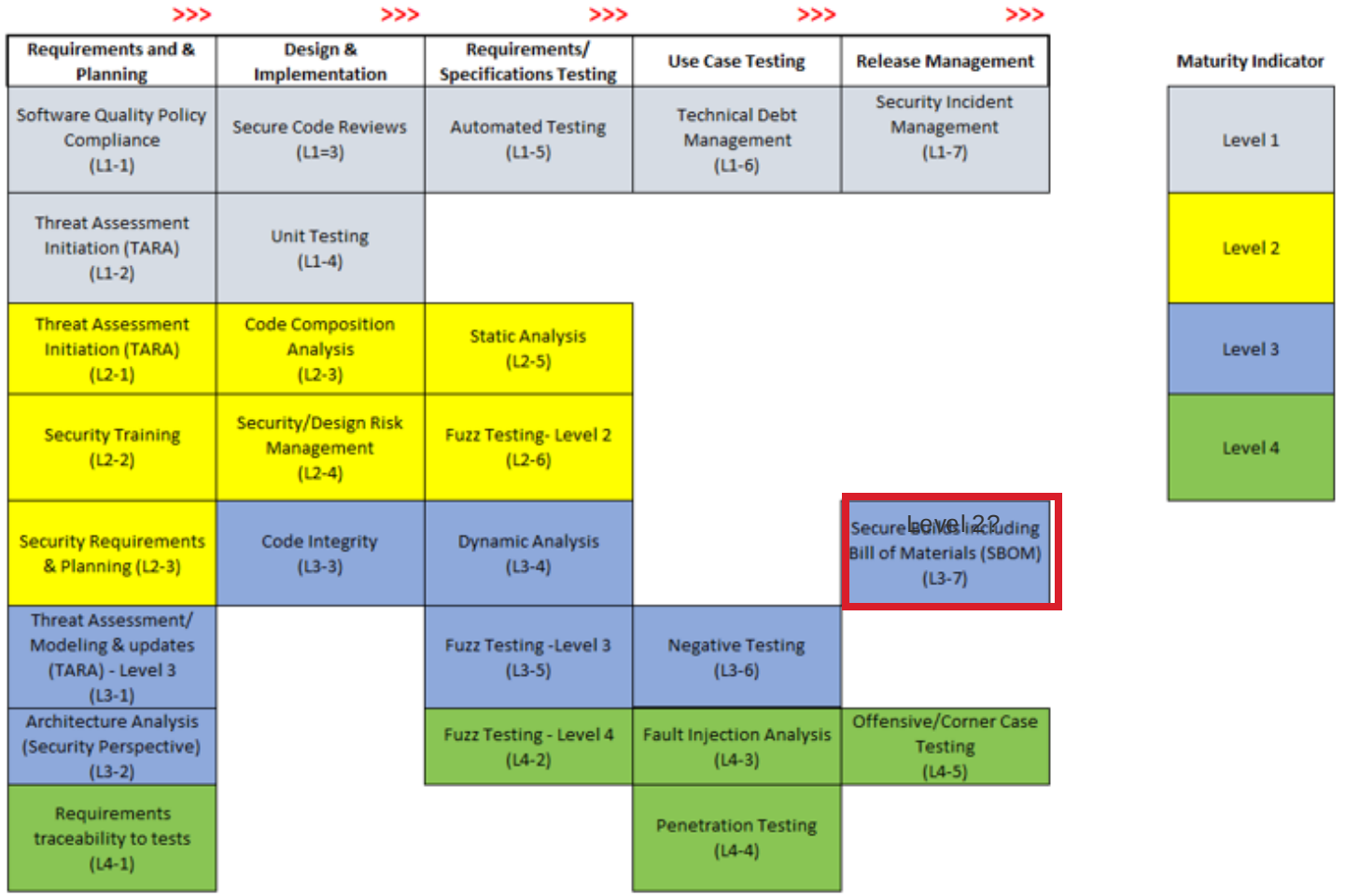
- PSIRT

- SBOM
- Security Certification

Secure By Design aligns well with Secure Software Development Lifecycle (SDLC)



A possible implementation of the Secure-SDLC Maturity Framework (SSMF)



You can then map Secure SDLC to Security Frameworks like ISO 27001

Secure SDLC Coverage Color Coding		Level 1 (B1-B7)	Level 2 (M1-M7)	Level 3 (P1-P7)	Level 4 (E1-E5)		
Mapping of Secure-SDLC to multiple standards Note that the standards listed with an asterisk(*) are only partially covered by Secure-SDLC.							
Topic/Clause	BSIMM (11)	NIST SSDF (800-218)	Common Criteria (Version 3.1 rev 5) or ISO/IEC 15408	ISO 27001 (2013)*	ISO/IEC 62443*	ISO/IEC 12207/24748-3*	ISO 9001* / QS4310, QS4320
Configuration/Settings Management	Architecture Analysis (AA1-AA3), Config. Mgmt. & Vuln. Mgmt. (CMVM1-CMVM3)	Configure Software to Have Secure Settings by Default (PW.9)	Security Assurance Components (7), Composed Assurance Packages (9), Class ACO:Composition (18)	A.14.2.5 Secure system engineering principles	Security guidelines (Clause 12 - Part 1), File Integration Security disposal guidelines (SG-4)	Configuration Management process (6.3.5)	Design & Development of products & services (8.3)
Efficiency & Modularity/ Redundancy reduction	Strategy & Metrics (SM1-SM3)	Implement Supporting Toolchains (PO.3), Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality (PW.4)	Class ALC: Life-Cycle Support (15), Class ACO:Composition (18)	Class ALC: Life-Cycle Support (15), Class ACO:Composition (18)	Annex A - Part 1 Dependent component or operating system security update documentation (SUM-3)	Infrastructure Management Process (6.2.2) Measurement process (6.3.7)	Continual Improvement (10.3)
Process Governance	Strategy & Metrics (SM1-SM3), Compliance & Policy (CP1-CP3), Standards & Requirements (SR1-SR3)	Define and Use Criteria for Software Security Checks (PO.4)	Class ACE: Protection Profile Configuration Evaluation (11), Security Target Evaluation (12), Class ALC: Life-Cycle Support (15)	9.2 Internal Audit, A.12.1.1 Documented operating procedures, A.12.1.2 Change management, A.14.2.1 Secure development policy, A.14.2.7 Outsourced development, A.17.1 Information security continuity, A.18.2.3 Technical compliance review	Process verification (SM-12), Continuous Improvement (SM-13) Secure coding standards (SI-2) Periodic review of security defect management practice (DM-6) Documentation review (SG-7)	Life Cycle Concepts (6.2) Quality Management Process (6.2.5) Transition Process (6.4.10)	Operational planning and control (8.1) Improvement (1)
Roles and Responsibilities	Strategy & Metrics (SM1-SM3)	Implement Roles and Responsibilities (PO.2)	Class AGD: Guidance documents	7.4 Communication, A.9.2 User access management	Identification of responsibilities (SM-2) Identification of Applicability (SM-3) Independence of Testers (SVV-5)	Technical Management Process (6.3) Stakeholder Needs and Requirements Definition process (6.4.2)	Organizational roles, responsibilities, and authorities (5.3) Resources-People (7.1.2)
Secure Coding Practices	Secure Code Review (CR1-CR3)	Create Source Code by Adhering to Secure Coding Practices (PW.5), Configure the Compilation, Interpreter, and Build Processes to Improve Executable Security (PW.6)	Class ALC: Life-Cycle Support (15)	A.18.2.3 Technical compliance review	Development Process (SM-1), Defense in depth design (SD-2) Secure Design Review (SD-3) Secure Design Review Best Practices (SD-4) Secure coding standards (SI-2)	Design Definition Process (6.4.5) Implementation Process (6.4.7)	Design & development of products & services (8.3)
Secure Environments for Development	Software Environment (SE1-SE-3)	Implement and Maintain Secure Environments for Software Development (PO.5)	Security Assurance Components (7), Class ACO:Composition (18)	A.14.1.1 Information security requirements analysis and specification, A.14.2.6 Secure development environment, A.11.1 Secure areas, A.14.2.8 System security testing	Development Environment Security (SM-7), Custom developed components for third-party (SM-10) Secure Implementation review (SI-1) Defense in depth measures expected in the environment (SG-2)	Architecture Definition Process, Design Definition Process (6.4.3) Operation Process (6.4.12)	Design & Development of products & services (8.3)

Software Bill of Materials (SBOM)

June 2022 - NIST IR 8425 – Requires an SBOM

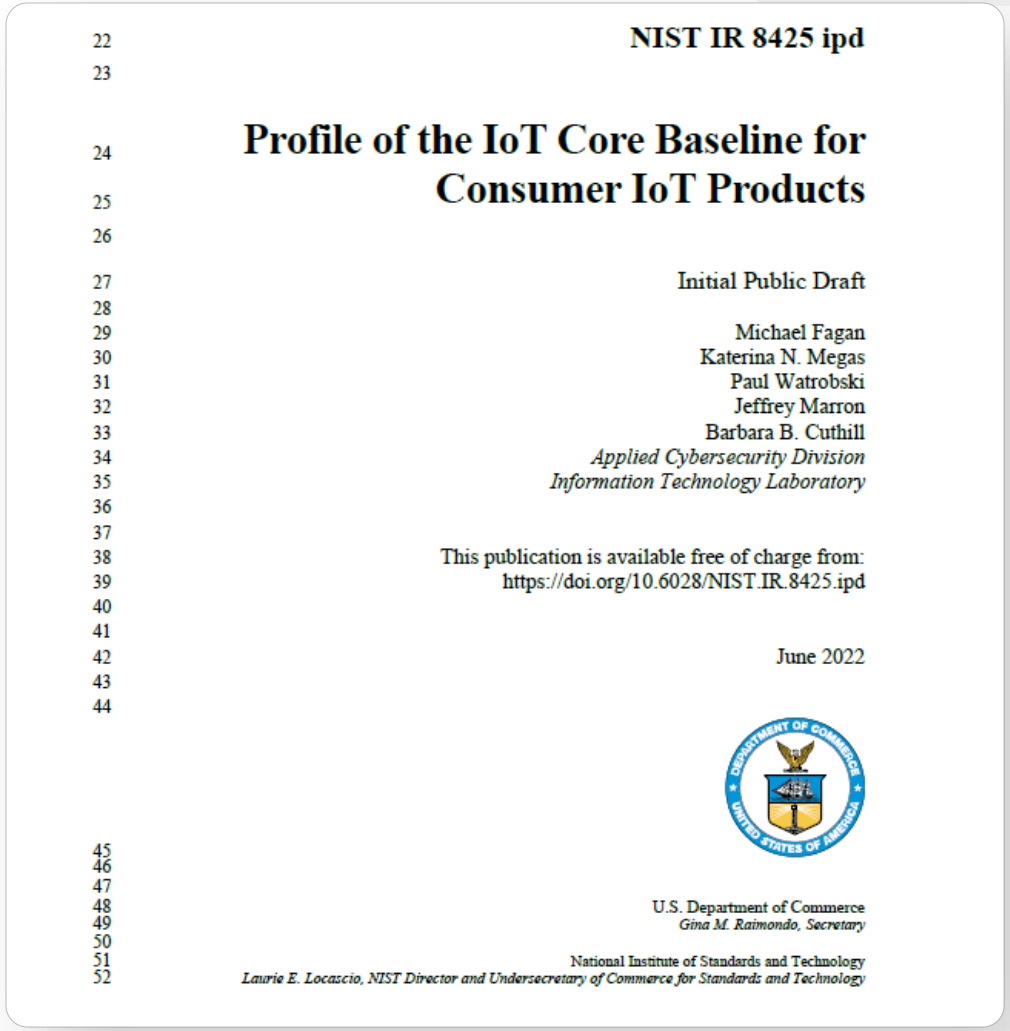
Documentation

The IoT product developer creates, gathers, and stores[6] information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.

1. Throughout the development lifecycle, the IoT product developer creates or gathers and stores information relevant to the cybersecurity of the IoT product and its product components, **including**:

    d. Product design and support considerations related to the IoT product, *for example*:
        i. All hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product (i.e., used to create each product component).

    f. The secure system lifecycle policies and processes associated with the IoT product, **including**:
        i. Steps taken during development to ensure the IoT product and its product components are free of any known, exploitable vulnerabilities.
        ii. The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.



NIST IR 8425 ipd

Profile of the IoT Core Baseline for Consumer IoT Products

Initial Public Draft

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

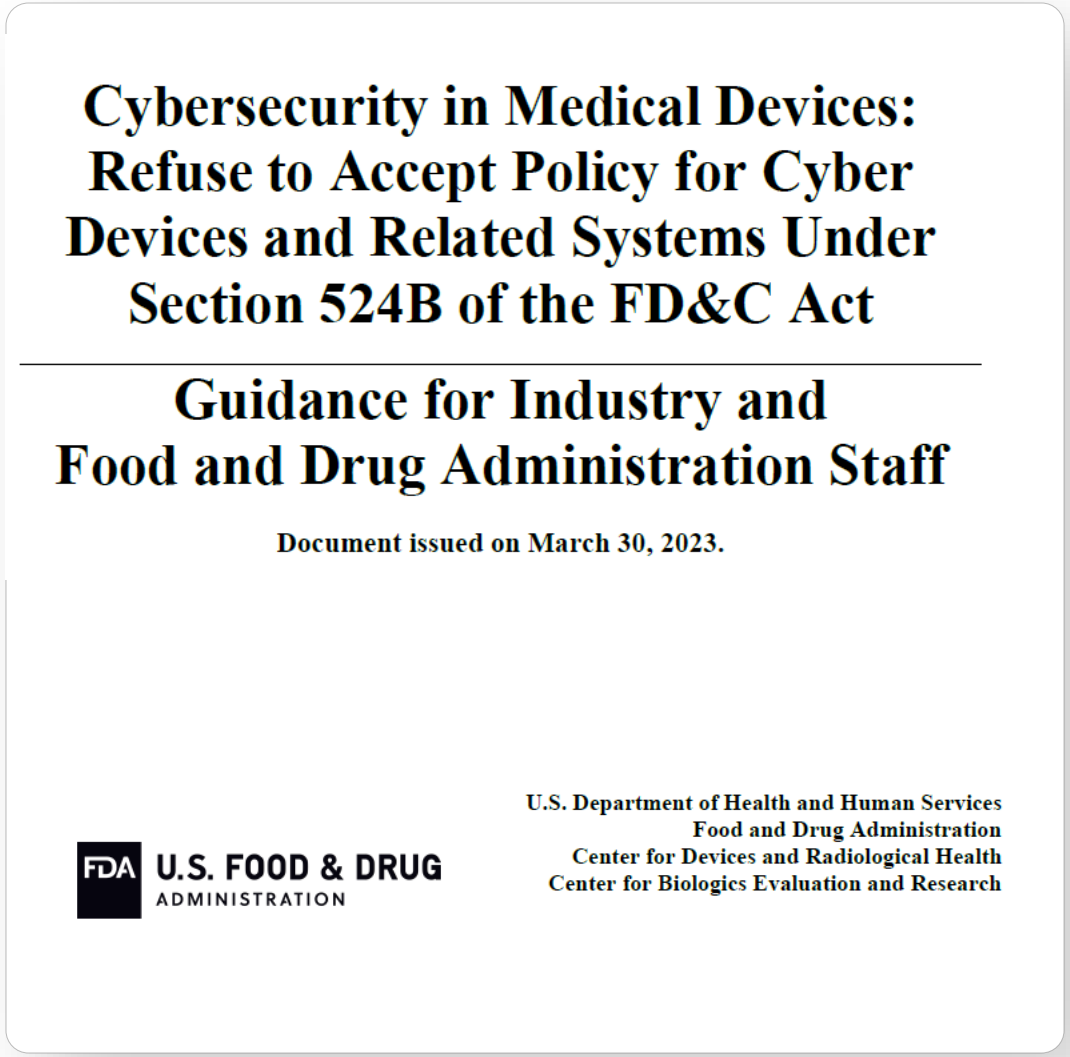
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425.ipd

June 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

March 30, 2023 - US Food and Drug (FDA) – Cybersecurity in Medical Devices will require an SBOM



Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act

Guidance for Industry and Food and Drug Administration Staff

Document issued on March 30, 2023.

U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

II.Policy

Effective March 29, 2023, the FD&C Act is amended to include section 524B "Ensuring Cybersecurity of Devices." Among section 524B's cybersecurity provisions are:

(a) IN GENERAL.—A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).

(b) The sponsor of an application or submission described in subsection (a) shall-

(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components;

RED - CENELEC Joint Technical Committee (JTC) 13 / Work Group (WG) 8 - Likely in effect in 2025

3 DOCUMENTS CURRENTLY BEING WORKED

Doc #	Radio Equipment Catagory
1	Internet connected radio equipment
2	Radio equipment that processes Personal, Traffic, or Location Data that is internet connected OR designed or intended for Childcare, Toys, or Wearables (even if non-internet connected)
3	Internet connected radio equipment that enables user to transfer, monetary value, or virtual currency

STANDARDIZATION REQUEST (SCOPE)

"… shall contain technical specifications that ensure… radio equipment, where applicable:

- Monitor and control network traffic
- Mitigate DOS attacks
- Up-to-date software without known vulnerabilities
- Secure mechanisms for updating software and firmware
- Protect exposed attack surfaces and minimize impact of attacks
- Protect personal and financial data at rest and during transit
- Inform users of changes that affect data protection and privacy
- Log internal activity that may affect security of the above
- Allow users to easily delete personal data

CURRENT MAIN REQUIREMENTS IN FEB 2023 DRAFT

Doc #	Security Function	Purpose
All	Access control mechanism	access control of resources
All	Authentication mechanism	the entity is what it claims to be
All	Secure Update mechanism	patch vulnerabilities
All	Secure storage mechanism	privileged data at rest
All	Secure communication mechanism	privileged data in motion
All	Confidential Cryptographic Keys	guidance on key size, use, and storage
All	General equipment capabilities	up-to-date software and hardware with no known "exploitable" vulnerabilities, no unnecessary external interfaces
All	Cryptography	shall use for Secure Update, Secure Storage, Secure Comms, CSP generation, etc.
1	Resilience mechanism	mitigate DOS attack and return to defined state after attack
1	Network monitoring mechanism	detect DOS and defend
1	Traffic control mechanism	source address validation
2	User notification mechanism	notify user of changes of privileged data
2	Deletion mechanism	deletion of privileged data
2,3	Logging mechanism	events that might impact privileged data

Cyber Resiliency Act (CRA) – Competes with RED - Likely in effect in 2025

SECURITY FUNCTIONS

- Designed, developed, and produced with appropriate level of security based on risk
- Delivered without any known vulnerabilities
- Based on Risk Assessment:
  - Secure by default
  - Protection from unauthorized access
  - Confidentiality and Integrity of data at rest and in motion
  - Security updates
  - Secured interfaces
  - Secured against of DOS attacks

PRODUCT PROCESS REQUIREMENTS

- Public security support policy and period of service (Security Warranty)
- Publicly available SBOM in machine-readable format
- Publicly identify, document, and remediate vulnerabilities free of charge
- Regular security reviews and testing
- Publicly available documentation on security use, how to apply security updates, and how to securely decommission the device

CYBER SECURITY REQUIREMENTS - ANNEXES 1-6

Brussels, 15.9.2022
COM(2022) 454

ANNEXES 1 to 6

ANNEXES

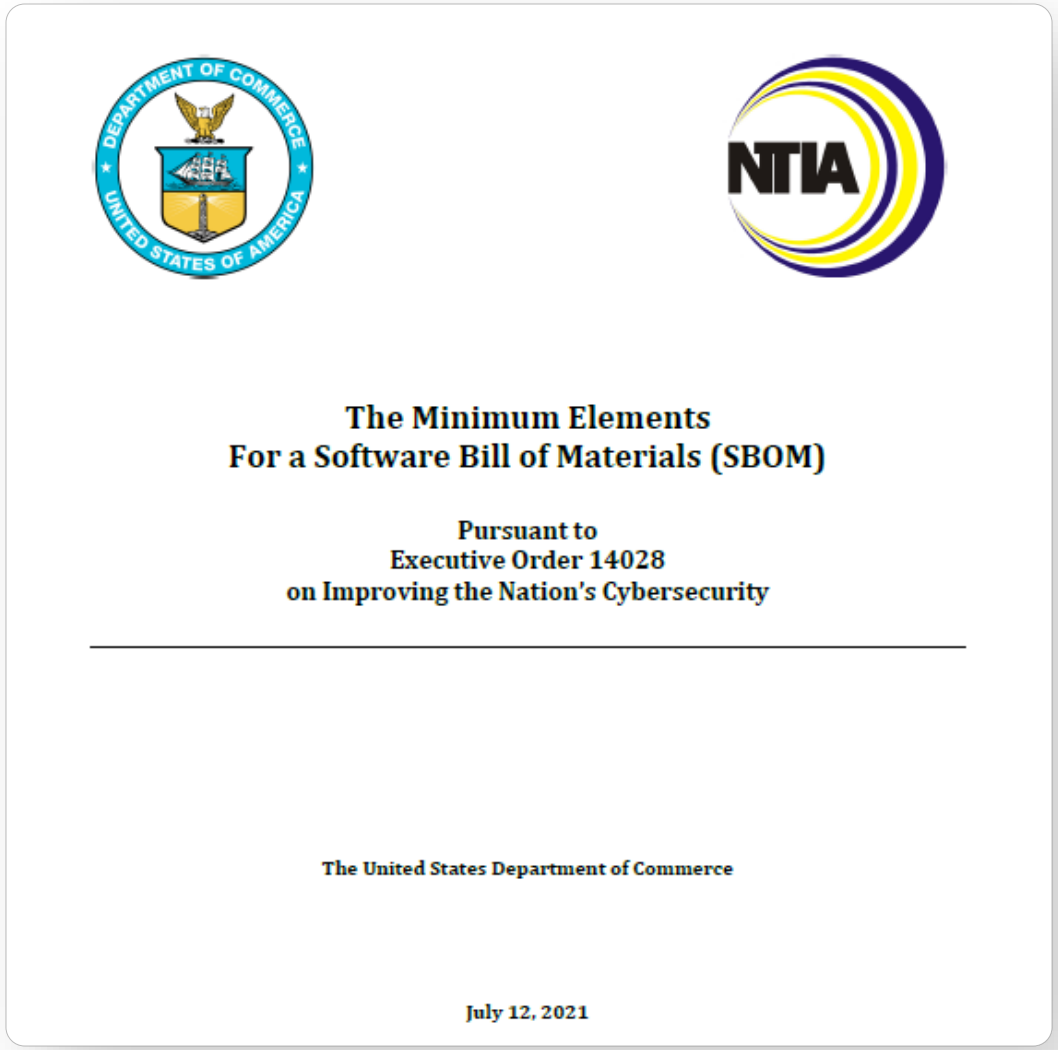
to the

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

{SEC(2022) 321} - {SWD(2022) 282} - {SWD(2022) 283}

National Telecommunications and Information Administration (NTIA) is driving the Standard for SBOMs https://ntia.gov/page/software-bill-materials



The Minimum Elements
For a Software Bill of Materials (SBOM)

Pursuant to
Executive Order 14028
on Improving the Nation's Cybersecurity

The United States Department of Commerce

July 12, 2021

The data formats that are being used to generate and consume SBOMs are:

- Software Package Data eXchange (SPDX)12
- CycloneDX13
- Software Identification (SWID) tags14

The SBOM must be conveyed across organizational boundaries in one of these interoperable formats.

Frequency. If the software component is updated with a new build or release, a new SBOM must be created to reflect the new version of the software.

Depth. An SBOM should contain all primary (top level) components, with all their transitive dependencies listed.

Known Unknowns. For instances in which the full dependency graph is not enumerated in the SBOM, the SBOM author must explicitly identify "known unknowns."

Distribution and Delivery. SBOMs should be available in a timely fashion to those who need them and must have appropriate access permissions and roles in place.

Summary

- Regulation timelines are accelerating and will be in full force in the next 1-2 years
- Once regulations are in place… the next frontier will be Certification processes to assure the requirements are being met
- Besides Requirements… the regulations are imposing development methodologies
  - “Secure by Design” which include public product incident response programs for a continuous feedback loop
  - Software Bill of Materials (SBOM)

Thank You