SILICON LABS

works with
BY SILICON LABS

IOT-101

Biggest Security Trends and What to Expect

Mike Dow | August 2023

IOT

Agenda

01 The World-Wide Security Regulation Landscape

02 Certification Processes… how they will assure compliance to the regulations

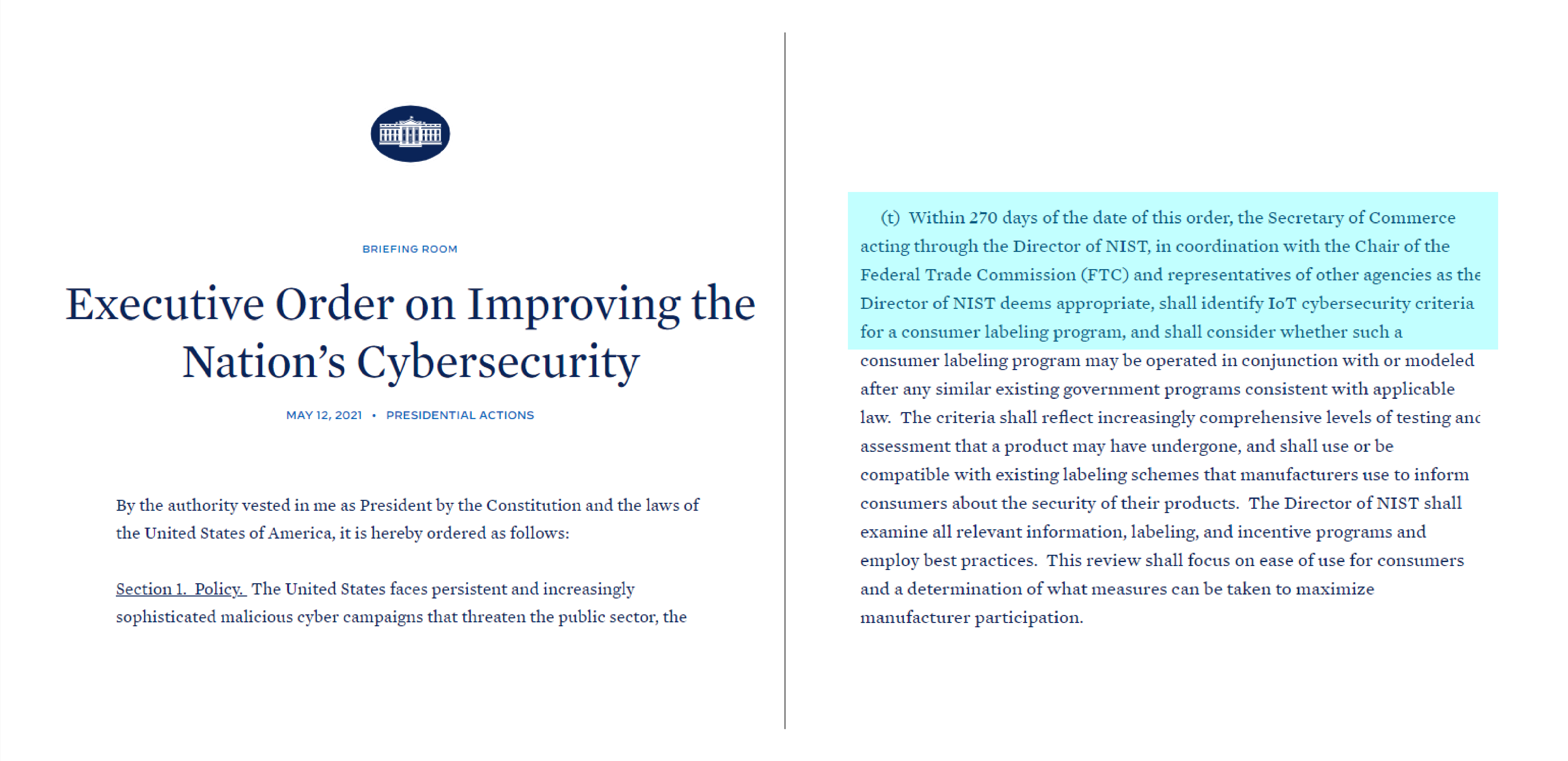
03 Secure Software Development Lifecycles (Secure SDLC)

04 Software Bill of Materials (SBOM)

works with
BY SILICON LABS

World-Wide Security Regulation Landscape

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



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

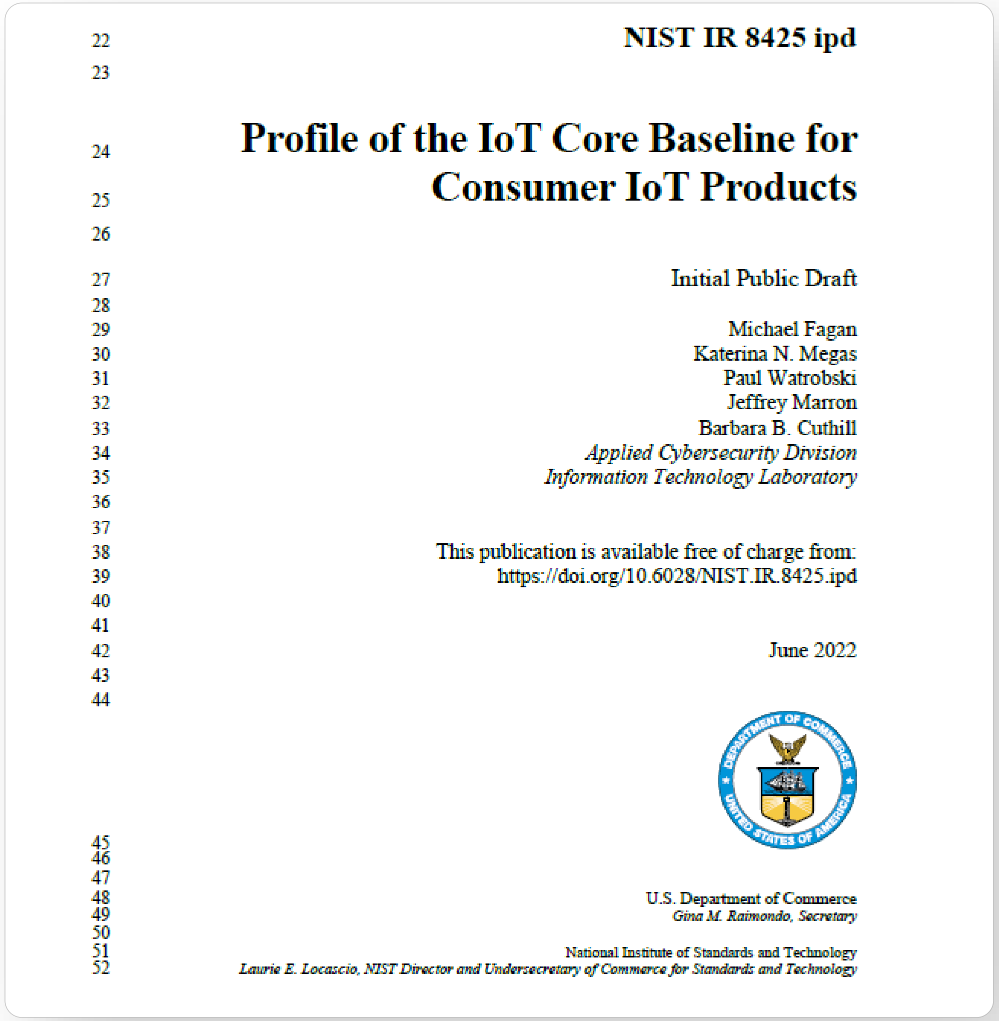
MAY 12, 2021 • PRESIDENTIAL ACTIONS

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

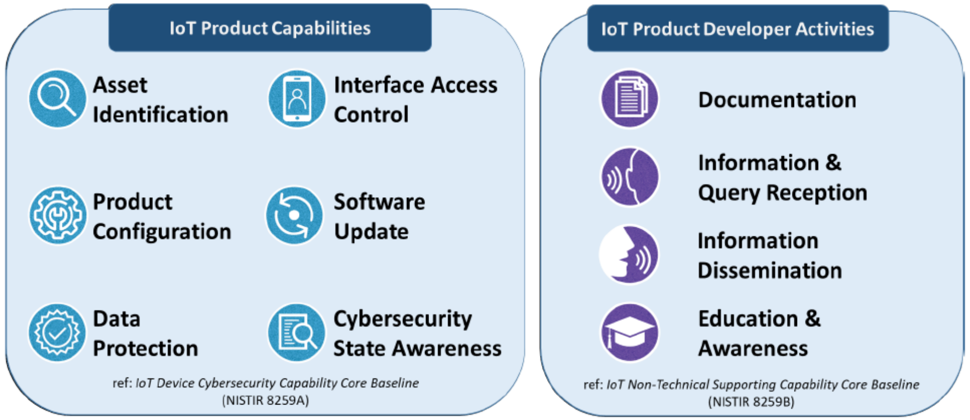
Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

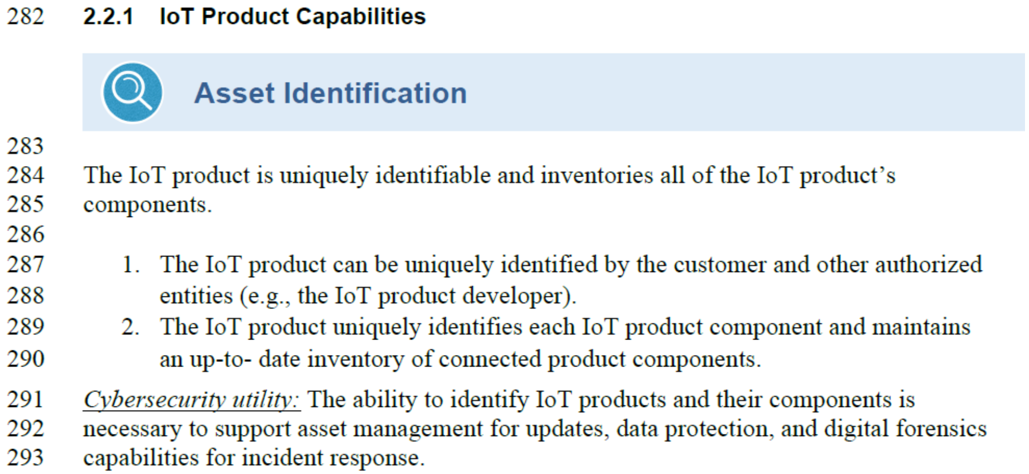
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425.ipd

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


IoT Product Capabilities
Asset Identification
Interface Access Control
Product Configuration
Software Update
Data Protection
Cybersecurity State Awareness
ref: IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A)
IoT Product Developer Activities
Documentation
Information & Query Reception
Information Dissemination
Education & Awareness
ref: IoT Non-Technical Supporting Capability Core Baseline (NISTIR 8259B)



2.2.1 IoT Product Capabilities

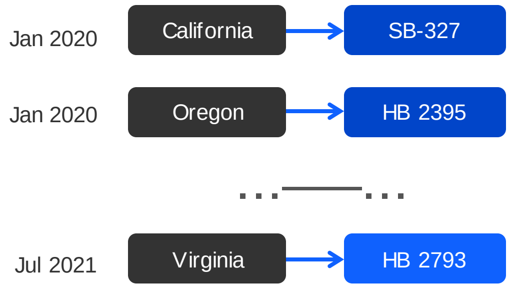
Asset Identification

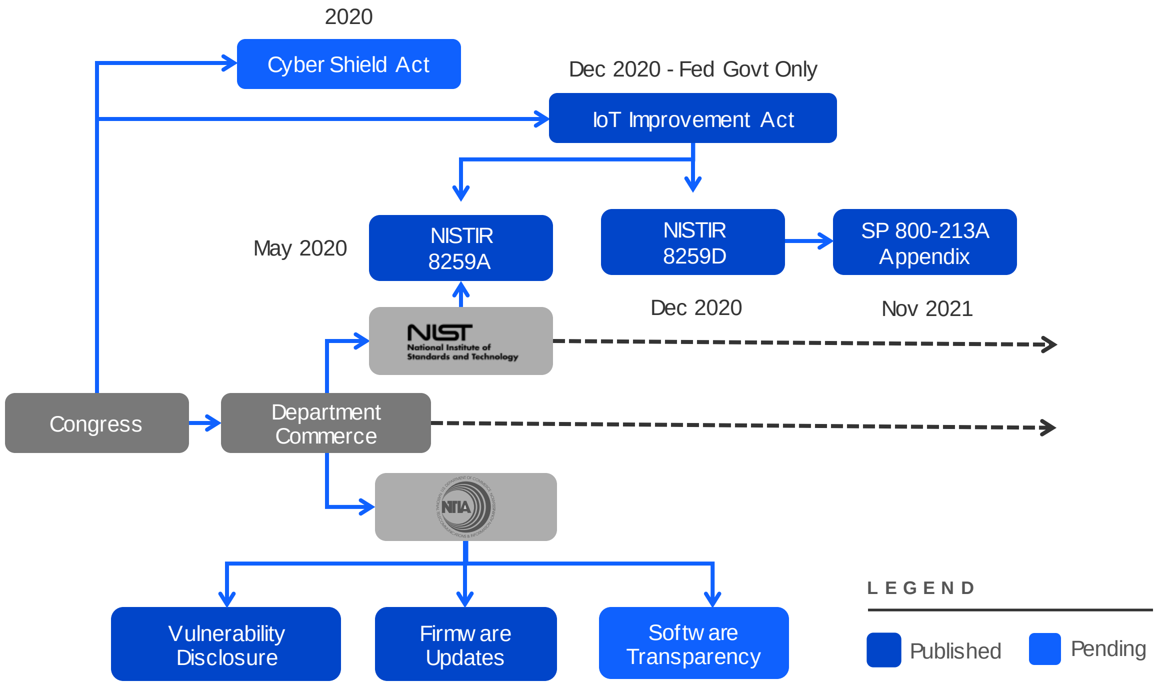
The IoT product is uniquely identifiable and inventories all of the IoT product's components.

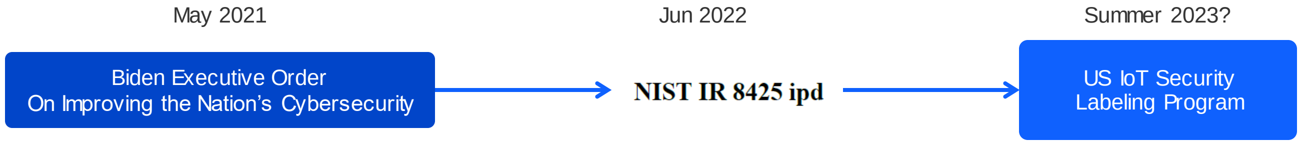
1. The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).
2. The IoT product uniquely identifies each IoT product component and maintains an up-to- date inventory of connected product components.

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.

Governmental Regulatory Landscape — United States



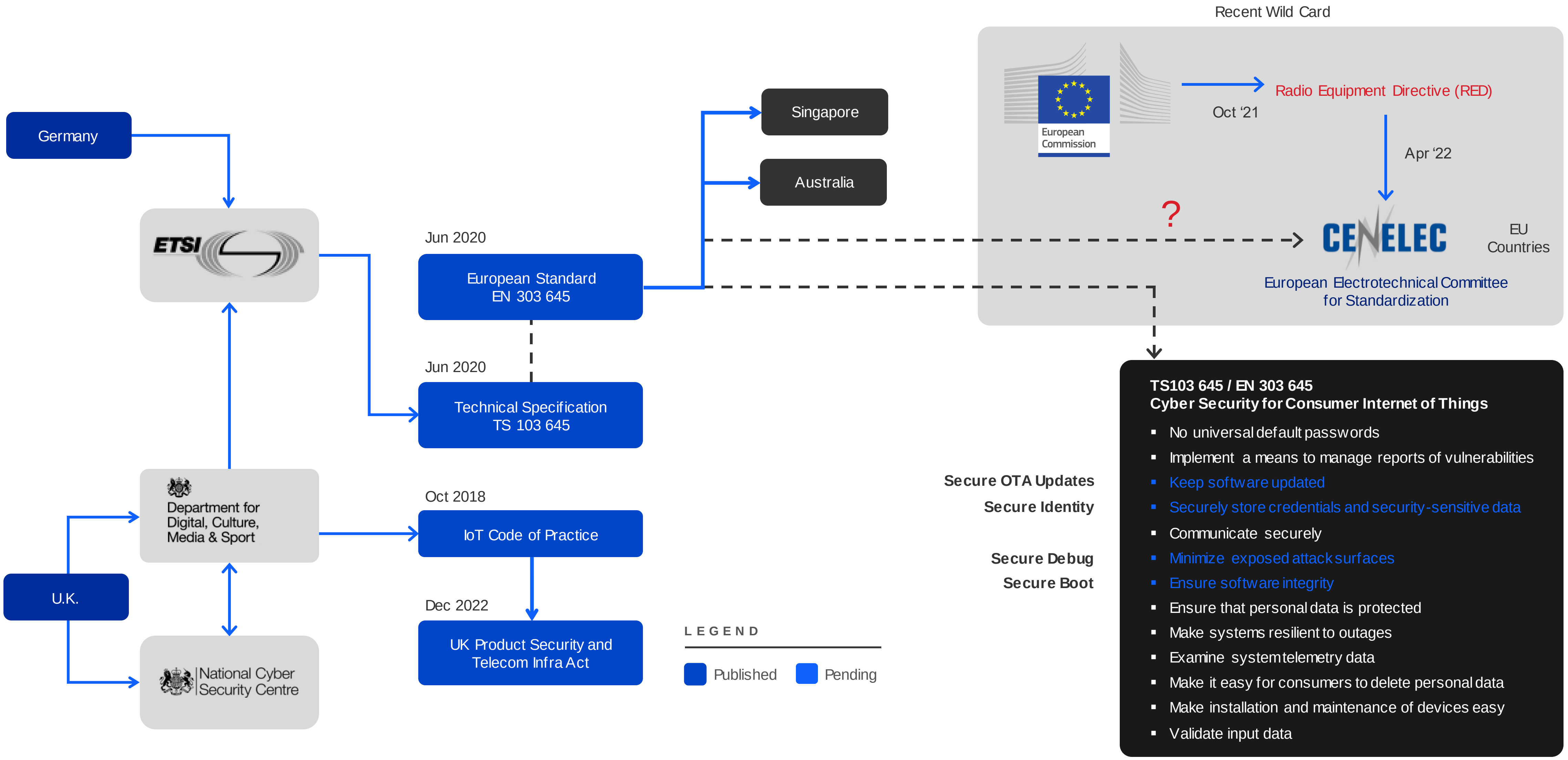



May 2021
Biden Executive Order On Improving the Nation's Cybersecurity
Jun 2022
NIST IR 8425 ipd
Summer 2023?
US IoT Security Labeling Program

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

Governmental Regulatory Landscape – Europe



Recent Wild Card
European Commission
Oct '21
Radio Equipment Directive (RED)
Apr '22
?
CENELEC
EU Countries
European Electrotechnical Committee for Standardization
Germany
ETSI
Singapore
Australia
Jun 2020
European Standard EN 303 645
Jun 2020
Technical Specification TS 103 645
Department for Digital, Culture, Media & Sport
U.K.
National Cyber Security Centre
Oct 2018
IoT Code of Practice
Dec 2022
UK Product Security and Telecom Infra Act
LEGEND
Published
Pending

TS103 645 / EN 303 645
Cyber Security for Consumer Internet of Things

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated — **Secure OTA Updates**
- Securely store credentials and security-sensitive data — **Secure Identity**
- Communicate securely
- Minimize exposed attack surfaces — **Secure Debug**
- Ensure software integrity — **Secure Boot**
- Ensure that personal data is protected
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

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)*

European Commission

EN English

Internal Market, Industry, Entrepreneurship and SMEs

Home > Sectors > Electrical and Electronic Engineering Industries (EEI) > Radio Equipment Directive (

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.**

CENELEC Joint Technical Committee (JTC) 13 / Work Group (WG) 8

TIMELINE

- Jul 7, 2022 - JTC 13/WG8 established
- Feb 2, 2023 – First Draft (complete)
- Sep 2023 – Acceptance of Final Version
- Sep 2023 - Submission to Formal Vote
- Nov 2023 – Closure of Formal Vote
- Dec 2023 – Ratification and Availability of Definitive Text **

** Note – If 5G included then June 2024

STANDARDIZATION REQUEST (SCOPE)

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

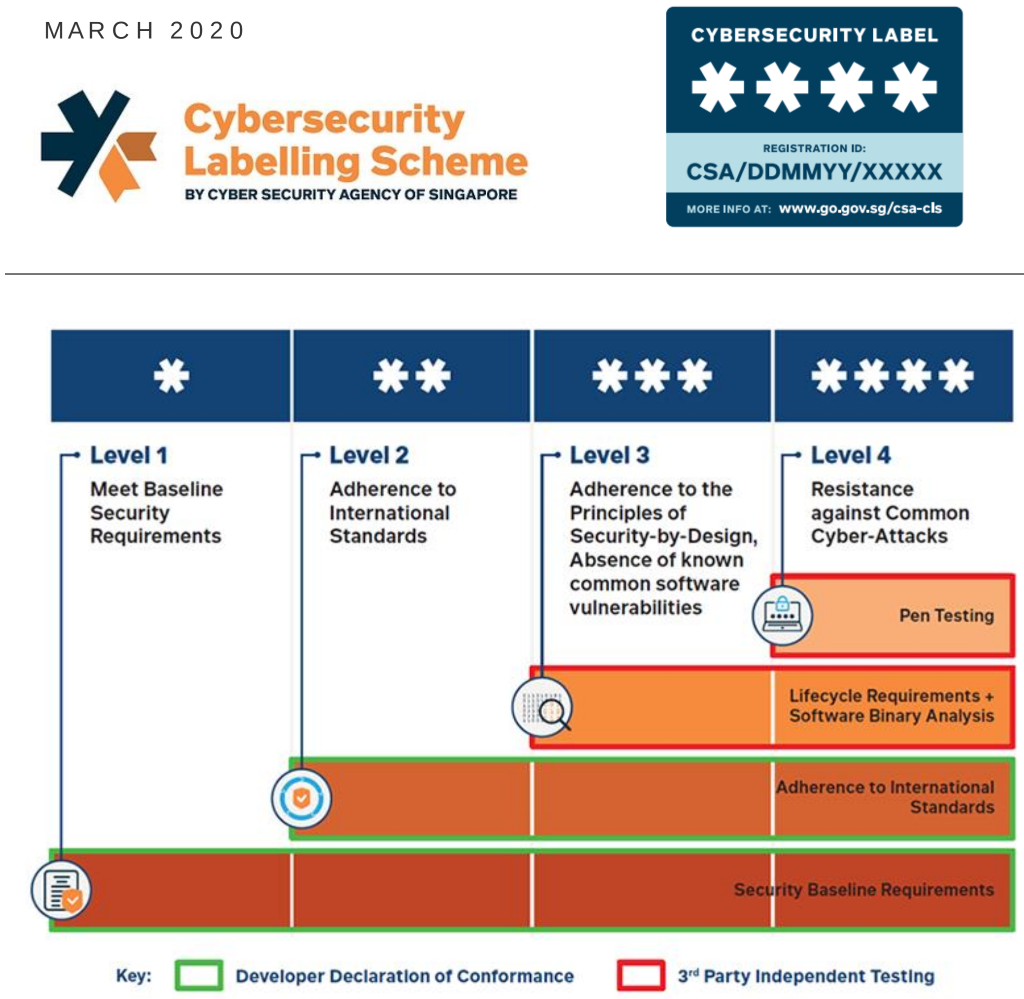
- Monitor and control network traffic
- Mitigate DOS attacks
- Up-to-date software without known vulnerabilities
- Secure mechanisms for updating software and firmware
- Protect exposed attack surfaces and minimize impact of attacks
- Protect personal and financial data at rest and during transit
- Inform 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

- Access control mechanism –> access control of resources
- Authentication mechanism –> the entity is what it claims to be
- Update mechanism –> patch vulnerabilities
- Secure storage mechanism –> privileged data at rest
- Secure communication mechanism –> privileged data in motion
- Logging mechanism -> events that might impact privileged data
- Deletion mechanism -> deletion of privileged data
- Resilience mechanism -> mitigate DOS attack and return to defined state after attack
- Attack surface reduction -> input validation
- Network monitoring mechanism -> detect DOS and defend
- Traffic control mechanism -> source address validation
- User notification mechanism -> notify user of changes of privileged data
- Critical Security Parameter (CSP) generation mechanism -> i.e. strong passwords, crypto keys, etc.
- General equipment capabilities – up-to-date software and hardware with no known "exploitable" vulnerabilities, no unnecessary external interfaces,
- Cryptography -> shall use for Secure Update, Secure Storage, Secure Comms, CSP generation, etc.

Singapore Cybersecurity Labeling Scheme (CSL)

Voluntary for now but will likely become mandatory



MARCH 2020

Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

CYBERSECURITY LABEL

✱✱✱✱

REGISTRATION ID:

CSA/DDMMYY/XXXXX

MORE INFO AT: www.go.gov.sg/csa-cls

✱	✱✱	✱✱✱	✱✱✱✱
Level 1 Meet Baseline Security Requirements	**Level 2** Adherence to International Standards	**Level 3** Adherence to the Principles of Security-by-Design, Absence of known common software vulnerabilities	**Level 4** Resistance against Common Cyber-Attacks

Pen Testing

Lifecycle Requirements + Software Binary Analysis

Adherence to International Standards

Security Baseline Requirements

Key: 🟩 Developer Declaration of Conformance 🟥 3rd Party Independent Testing

- 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

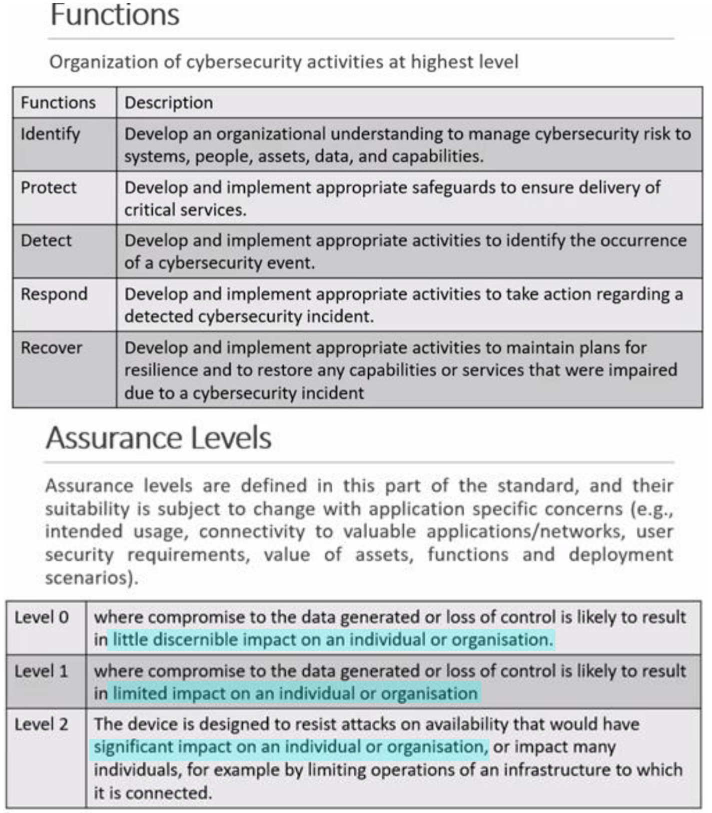
India IoT Standards

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
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
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

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.

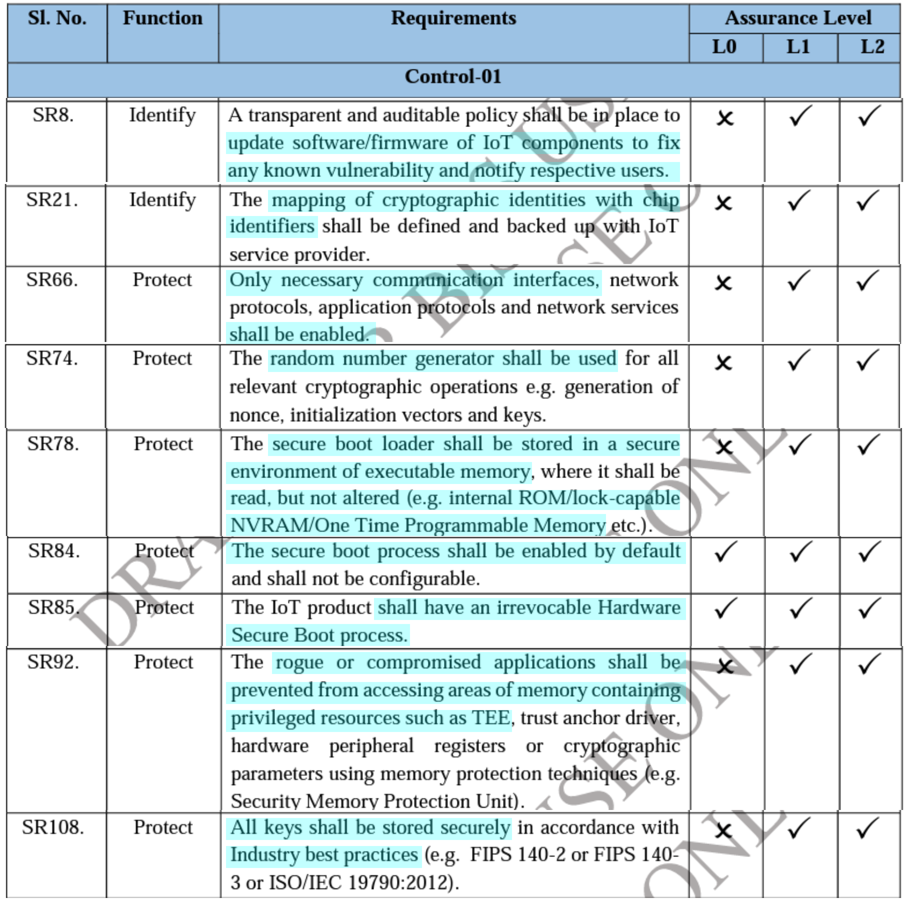
of Requirements
42
143
304
10
26

Total: 525

मानकः पथप्रदर्शकः

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).	✗	✓	✓

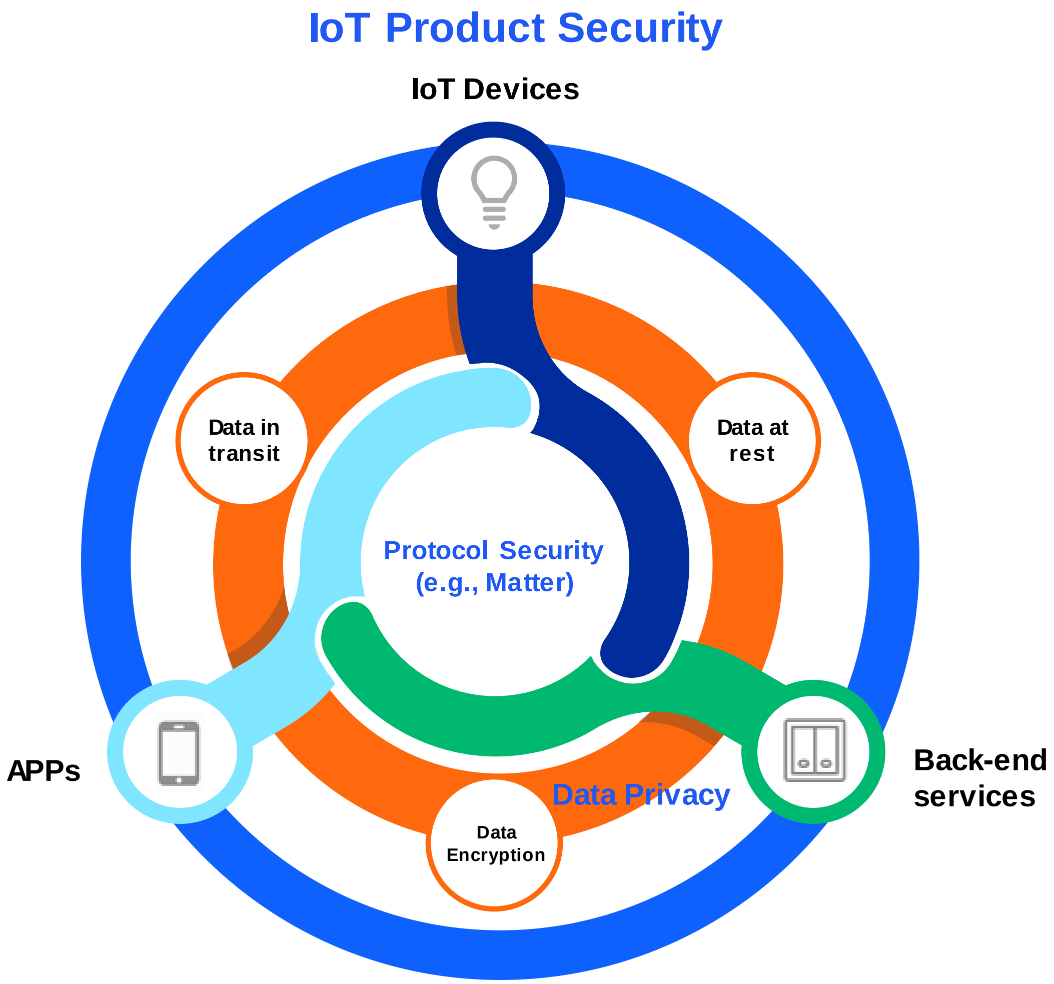
works with
BY SILICON LABS

Certification Processes

EXAMPLE

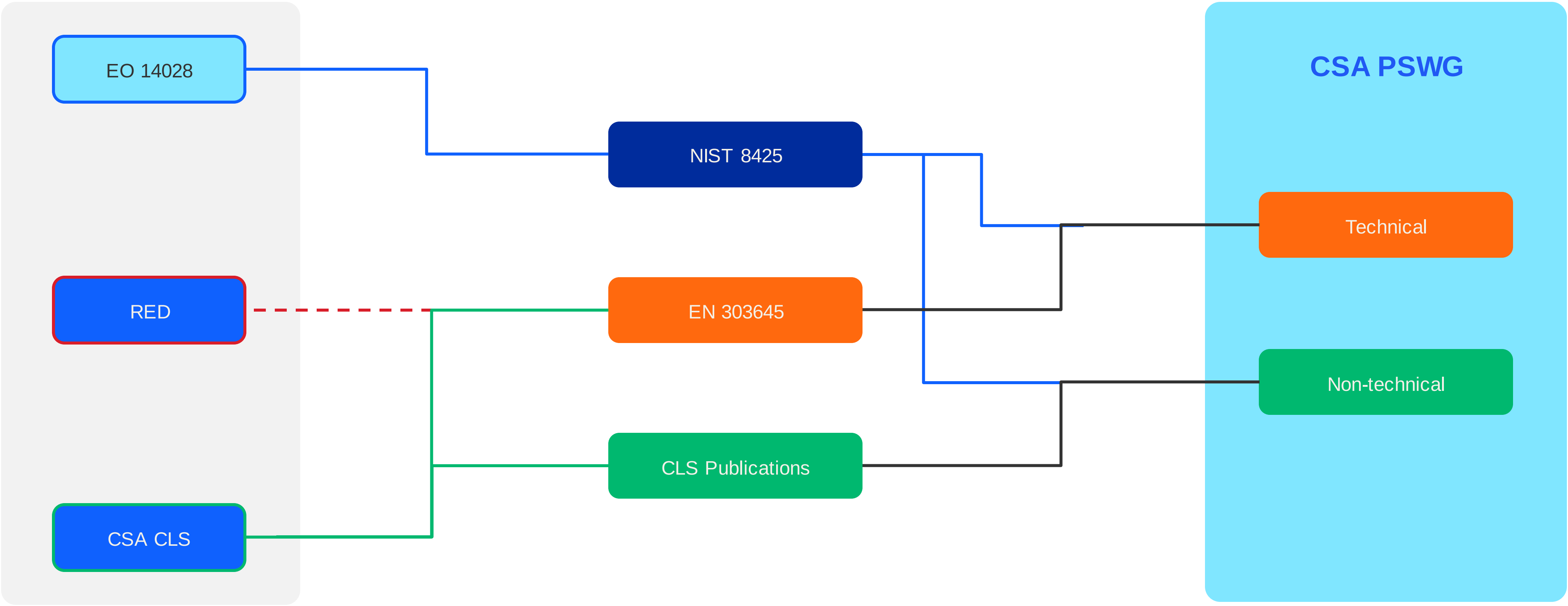
Connectivity Standards Alliance (CSA) Product Security Certification

Protocol Security vs. Product Security

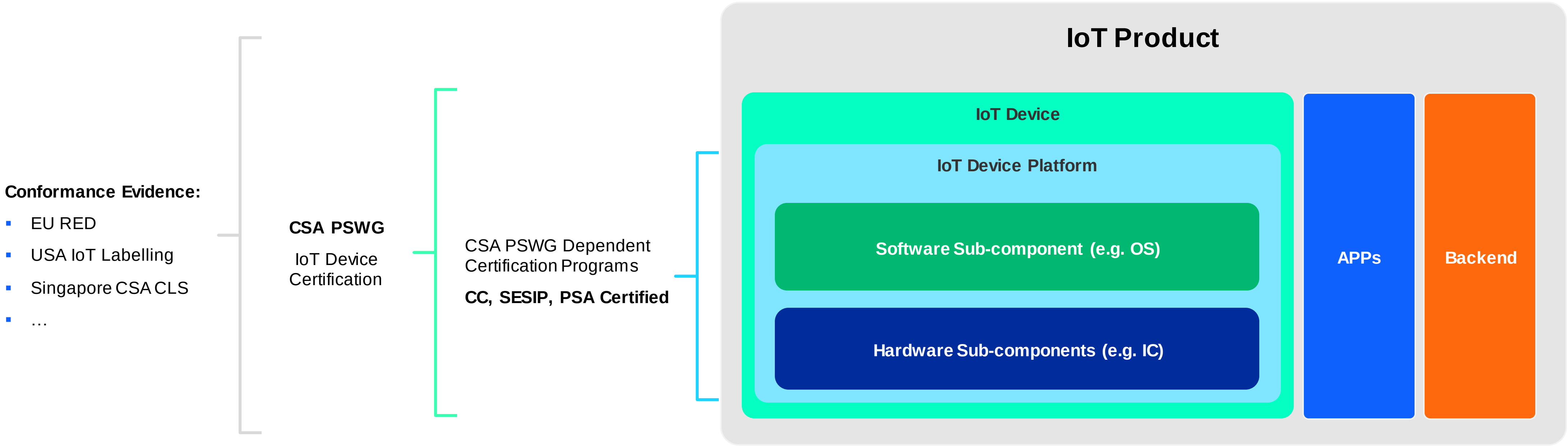


First Baseline Tech Spec Approved – v0.7 - June 2023

Full Certification Program by 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

IoT Product

IoT Device

IoT Device Platform

Software Sub-component (e.g. OS)

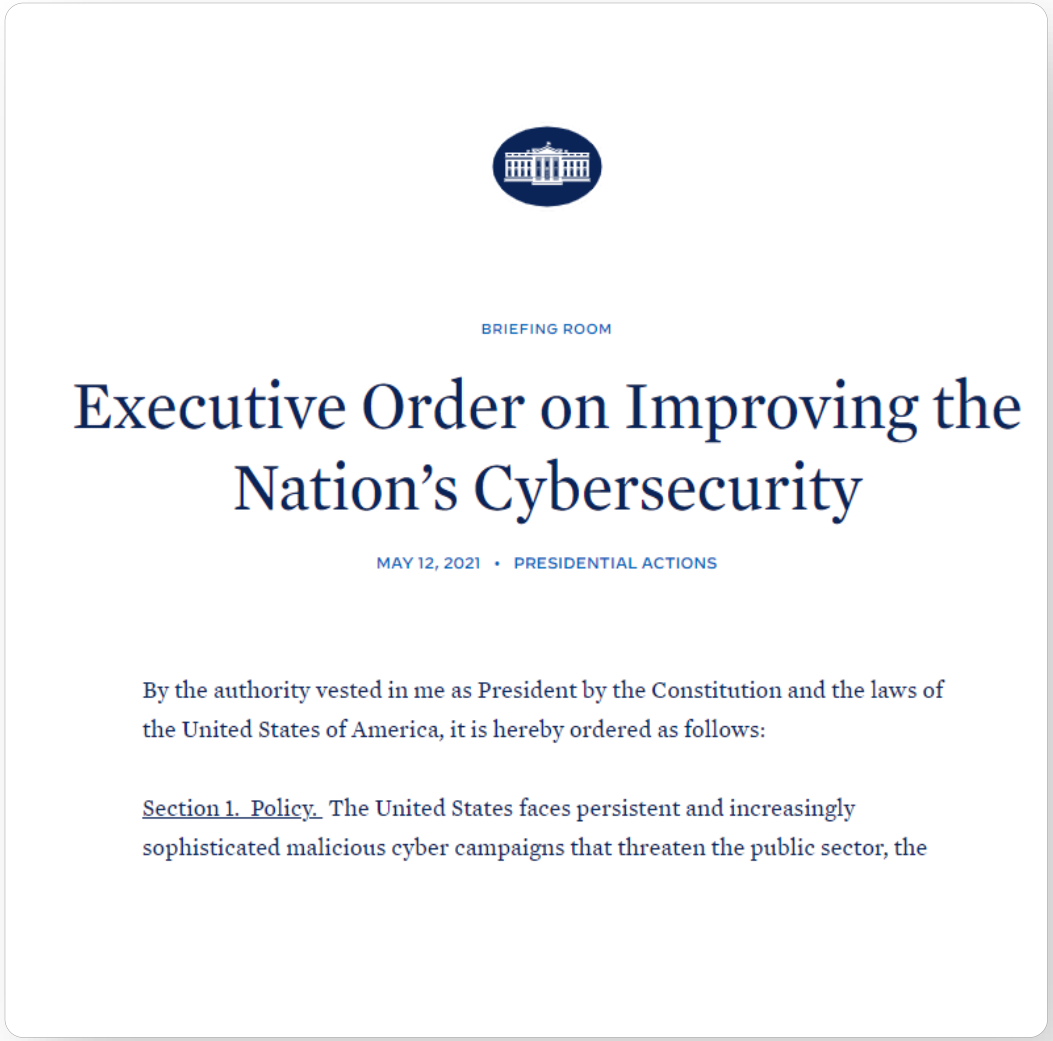
Hardware Sub-components (e.g. IC)

APPs

Backend

Secure Software Development Lifecycle (SDLC)

US Government contracts will require SDLC



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

(i) secure software development environments, including such actions as:

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

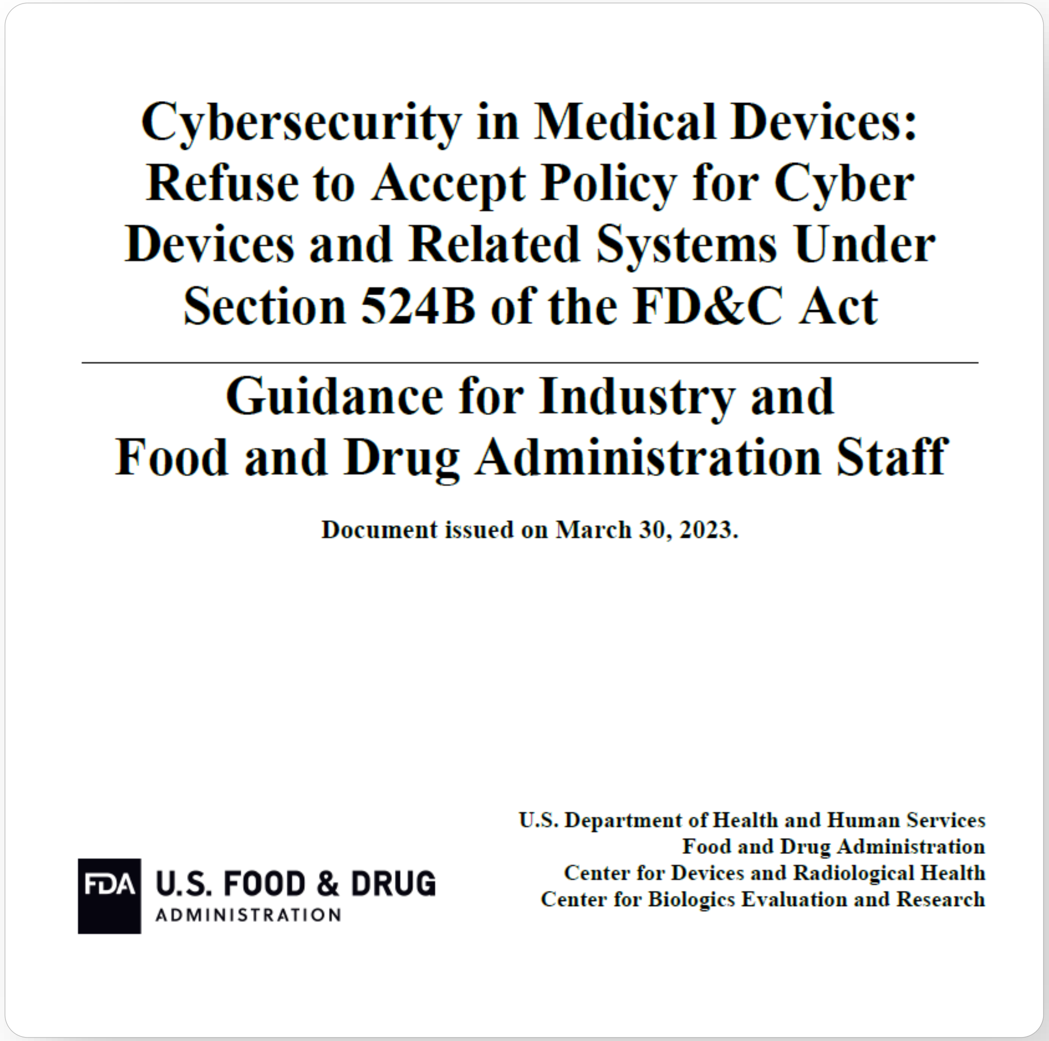
(ix) attesting to conformity with secure software development practices; and

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open-source software used within any portion of a product.

(r)…NIST…shall publish guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).

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.

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

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-

(1) submit to the Secretary a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;

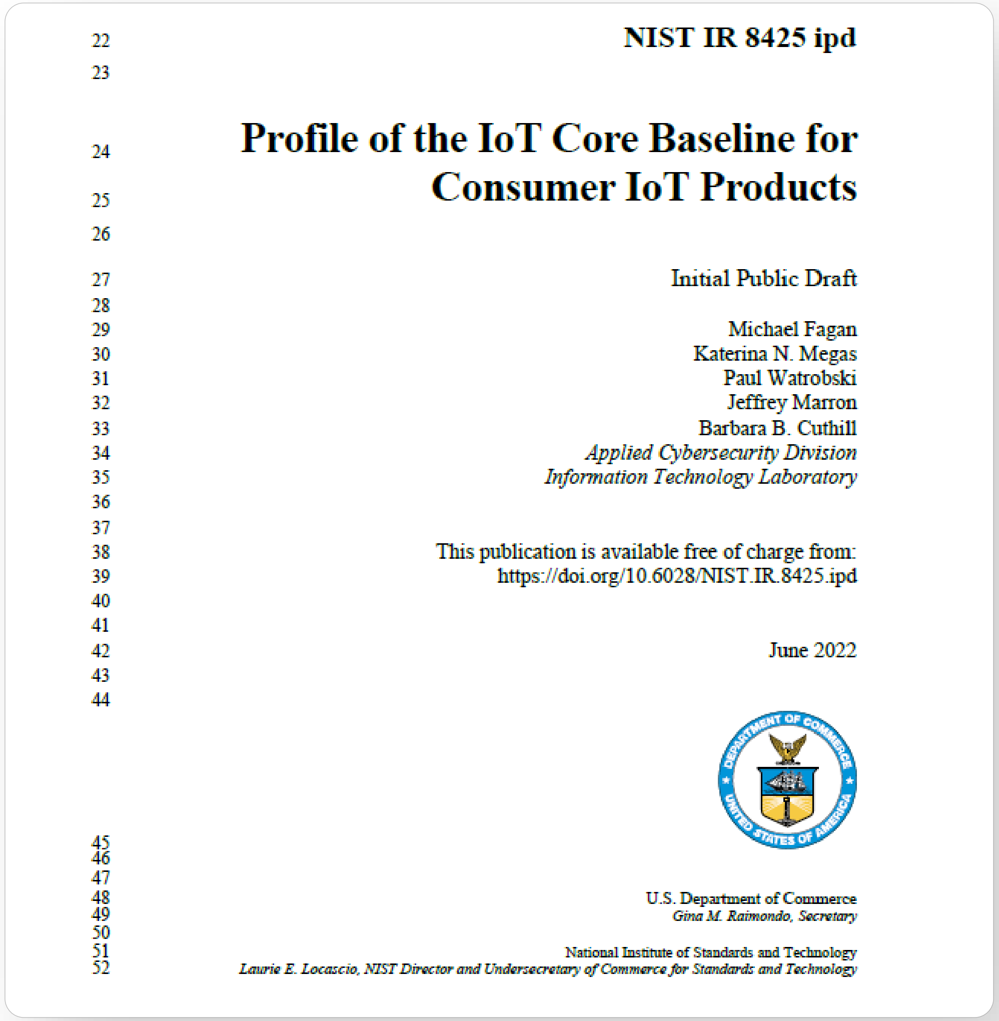
(2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecurity, and make available postmarket updates and patches to the device and related systems to address—

(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;

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

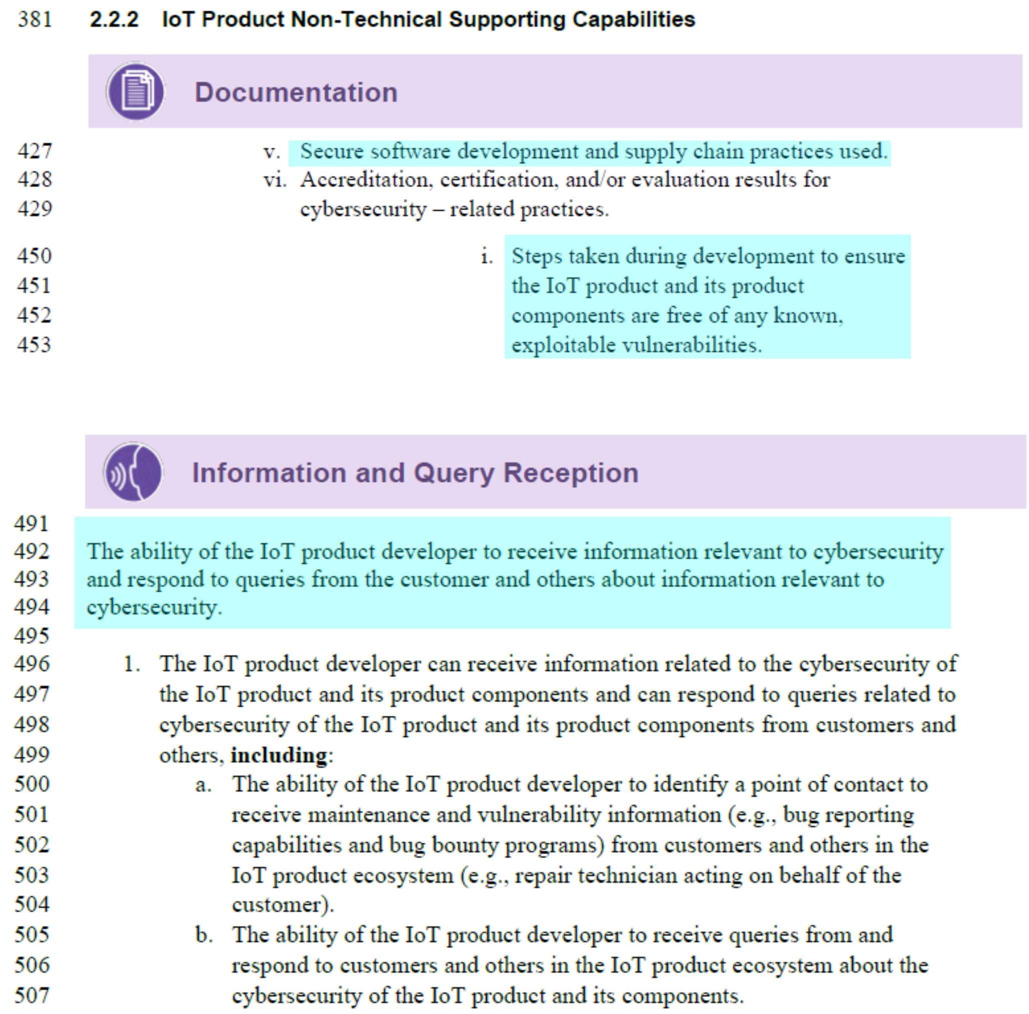
Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

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.

Singapore Cybersecurity Labeling Scheme (CSL)

Voluntary for now but will likely become mandatory

MARCH 2020

Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

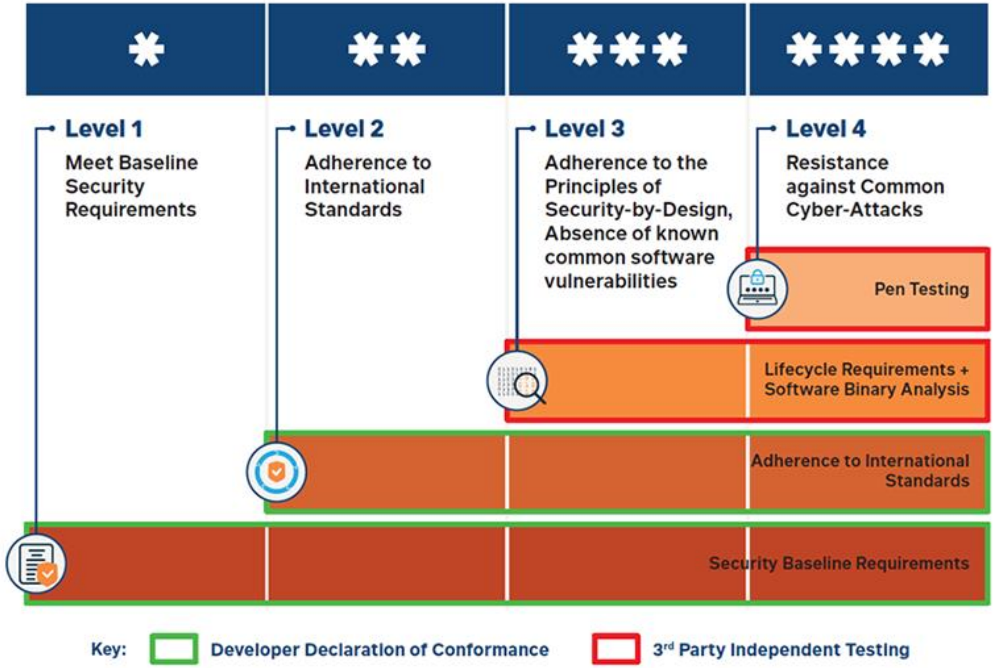
CYBERSECURITY LABEL

✱✱✱✱

REGISTRATION ID:

CSA/DDMMYY/XXXXX

MORE INFO AT: www.go.gov.sg/csa-cls


✱	✱✱	✱✱✱	✱✱✱✱
Level 1 Meet Baseline Security Requirements	**Level 2** Adherence to International Standards	**Level 3** Adherence to the Principles of Security-by-Design, Absence of known common software vulnerabilities	**Level 4** Resistance against Common Cyber-Attacks

Pen Testing

Lifecycle Requirements + Software Binary Analysis

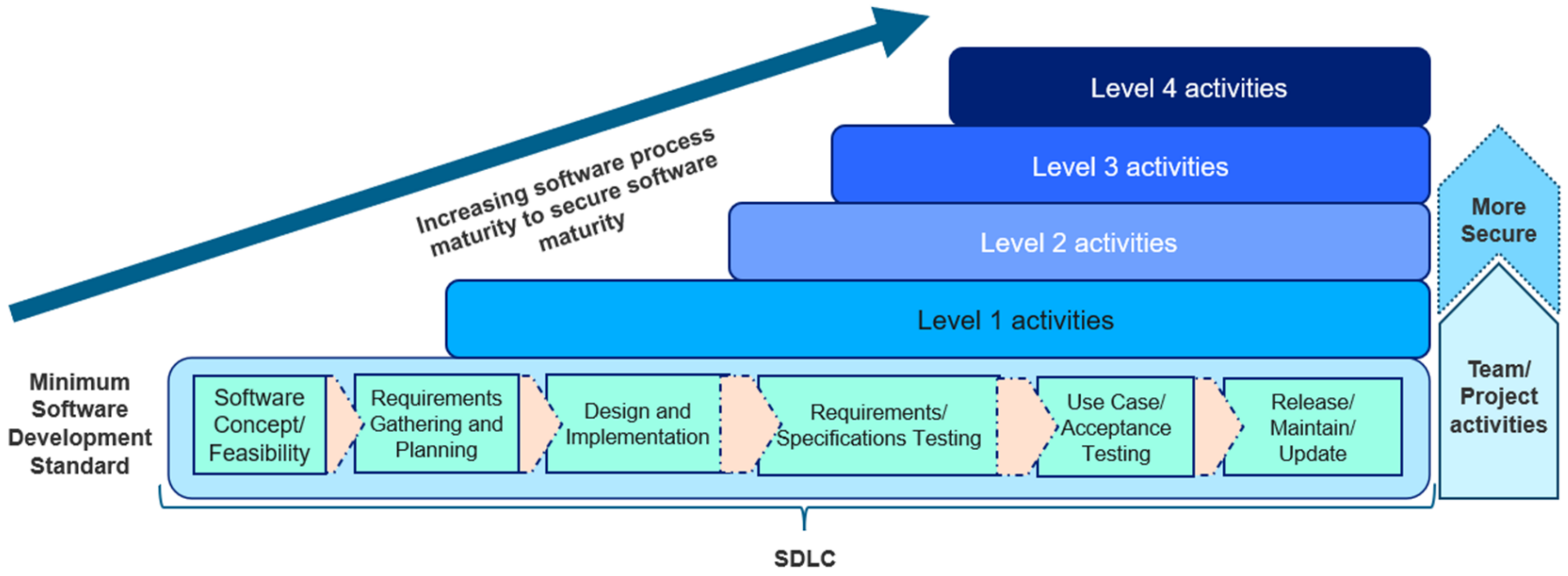
Adherence to International Standards

Security Baseline Requirements

Key: 🟩 Developer Declaration of Conformance 🟥 3rd Party Independent Testing

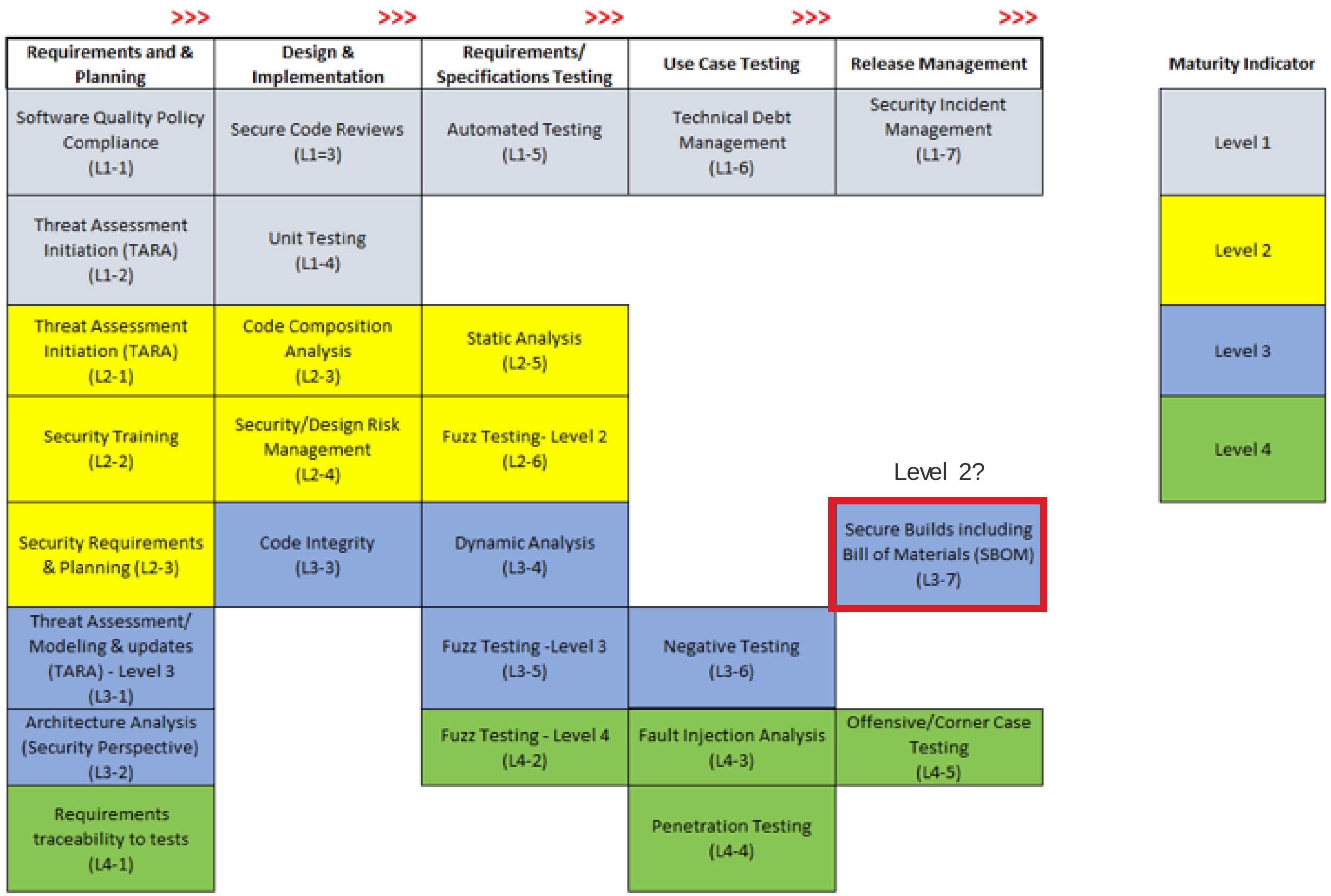
- Level 1 (Self Assessment)
  - No Universal Passwords
  - Report Vulnerabilities
  - Keep Software Securely Updated
- Level 2 (Self Assessment)
  - Meet all selected ETSI 303 645 Requirements
- Level 3 (Level 2 + Lab Verification)
  - Secure By Design
    - Threat Modeling
    - Secure by Design (Software/Hardware)
    - 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

Cumulative approach and alignment with SDLC



Increasing software process maturity to secure software maturity
Level 4 activities
Level 3 activities
Level 2 activities
Level 1 activities
More Secure
Team/ Project activities
Minimum Software Development Standard
Software Concept/ Feasibility
Requirements Gathering and Planning
Design and Implementation
Requirements/ Specifications Testing
Use Case/ Acceptance Testing
Release/ Maintain/ Update
SDLC

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



>>> >>> >>> >>> >>>

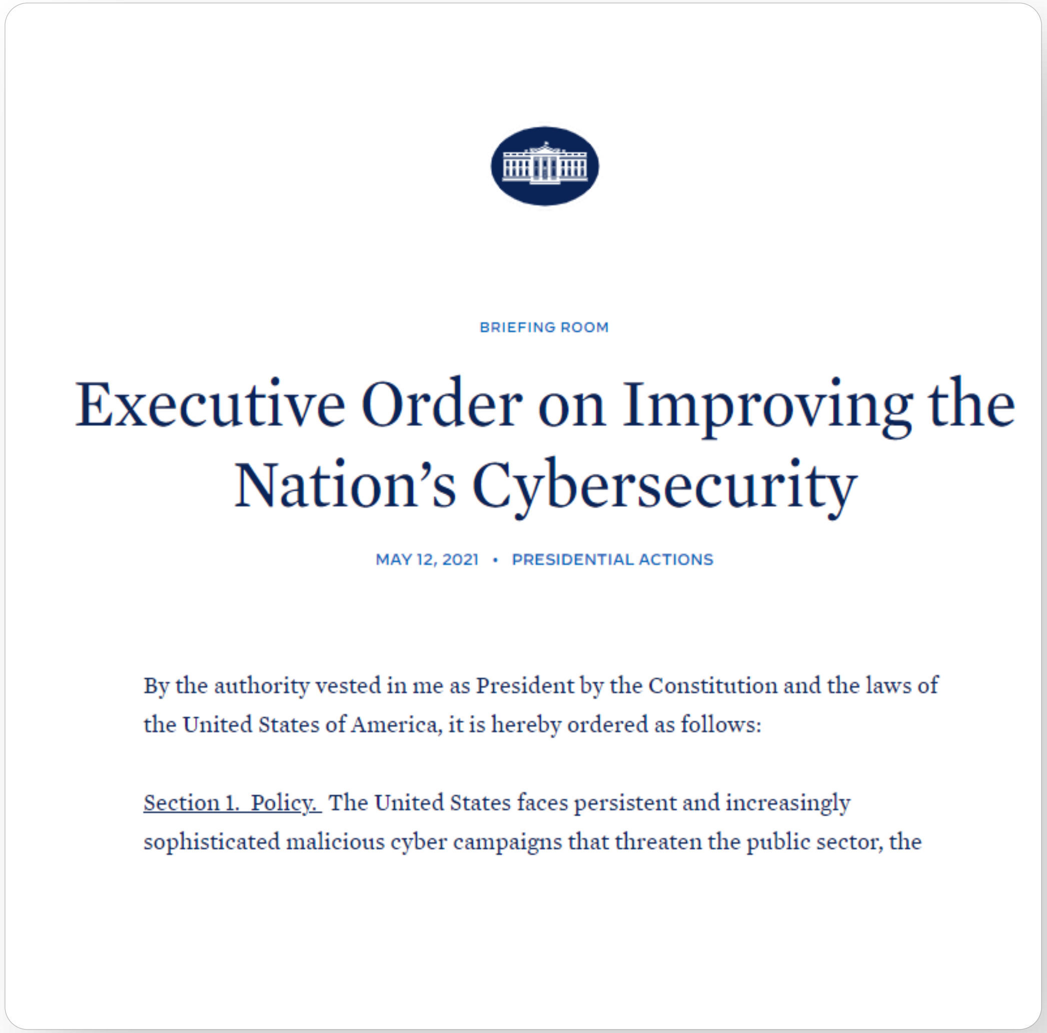
Requirements and & Planning	Design & Implementation	Requirements/ Specifications Testing	Use Case Testing	Release Management
Software Quality Policy Compliance (L1-1)	Secure Code Reviews (L1=3)	Automated Testing (L1-5)	Technical Debt Management (L1-6)	Security Incident Management (L1-7)
Threat Assessment Initiation (TARA) (L1-2)	Unit Testing (L1-4)			
Threat Assessment Initiation (TARA) (L2-1)	Code Composition Analysis (L2-3)	Static Analysis (L2-5)		
Security Training (L2-2)	Security/Design Risk Management (L2-4)	Fuzz Testing- Level 2 (L2-6)		Level 2?
Security Requirements & Planning (L2-3)	Code Integrity (L3-3)	Dynamic Analysis (L3-4)		Secure Builds including Bill of Materials (SBOM) (L3-7)
Threat Assessment/ Modeling & updates (TARA) - Level 3 (L3-1)		Fuzz Testing -Level 3 (L3-5)	Negative Testing (L3-6)	
Architecture Analysis (Security Perspective) (L3-2)		Fuzz Testing - Level 4 (L4-2)	Fault Injection Analysis (L4-3)	Offensive/Corner Case Testing (L4-5)
Requirements traceability to tests (L4-1)			Penetration Testing (L4-4)	

Maturity Indicator
Level 1
Level 2
Level 3
Level 4

works with
BY SILICON LABS

Software Bill of Materials (SBOM)

US Contracts will require an SBOM



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

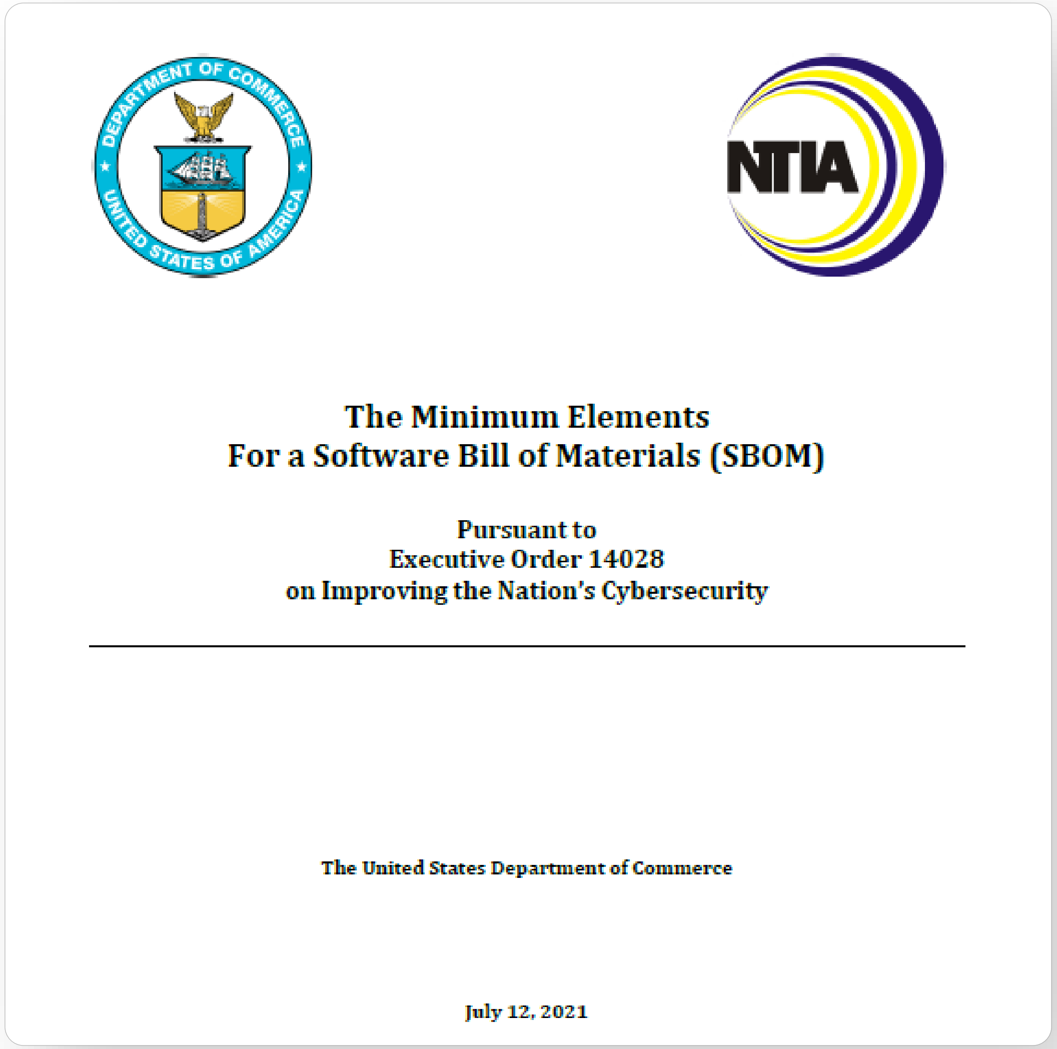
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

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

(vii) providing a purchaser, a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(f) …the Secretary of Commerce, …and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

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.

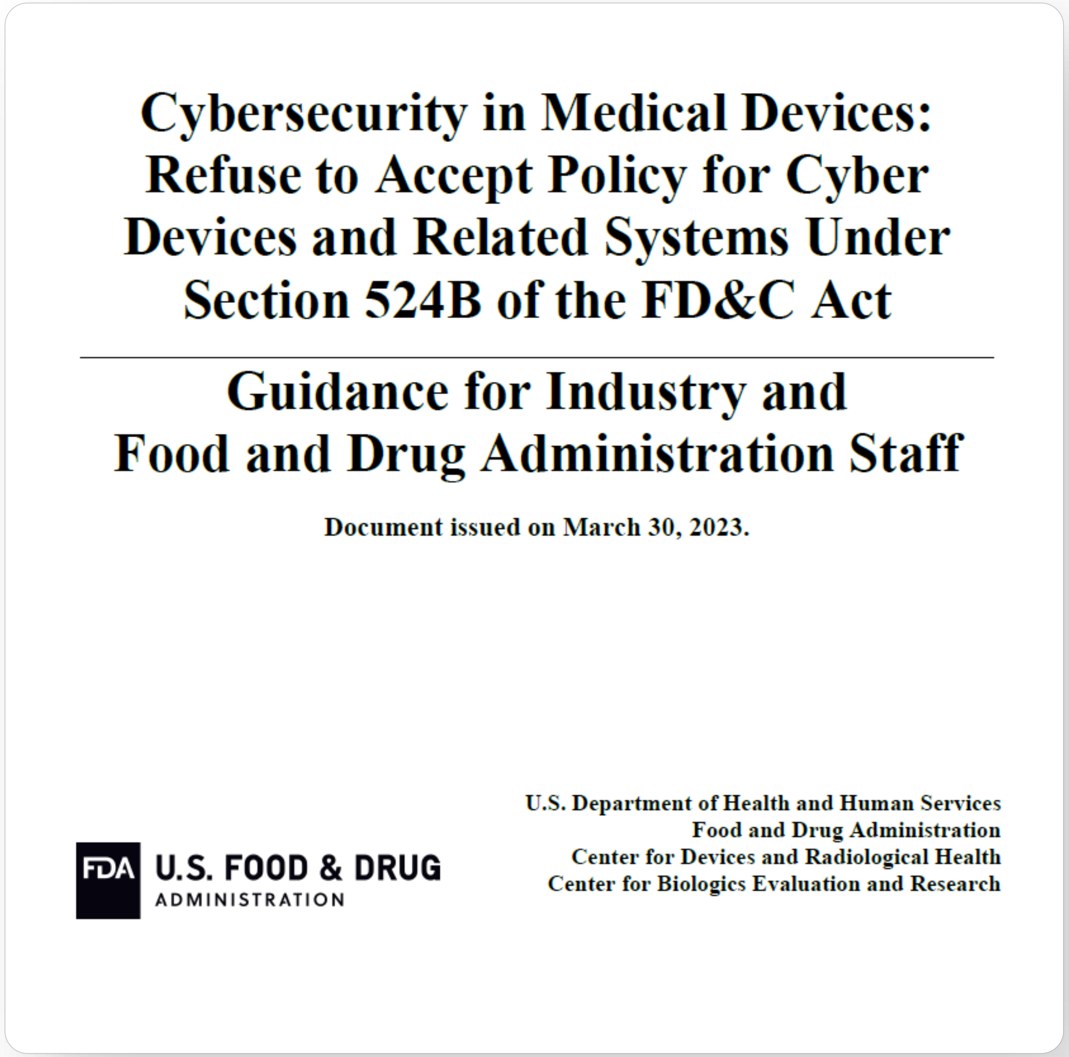
Frequency. If the software component is updated with a new build or release, a new SBOM must be created to reflect the new version of the software.

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.

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

FDA U.S. FOOD & DRUG ADMINISTRATION

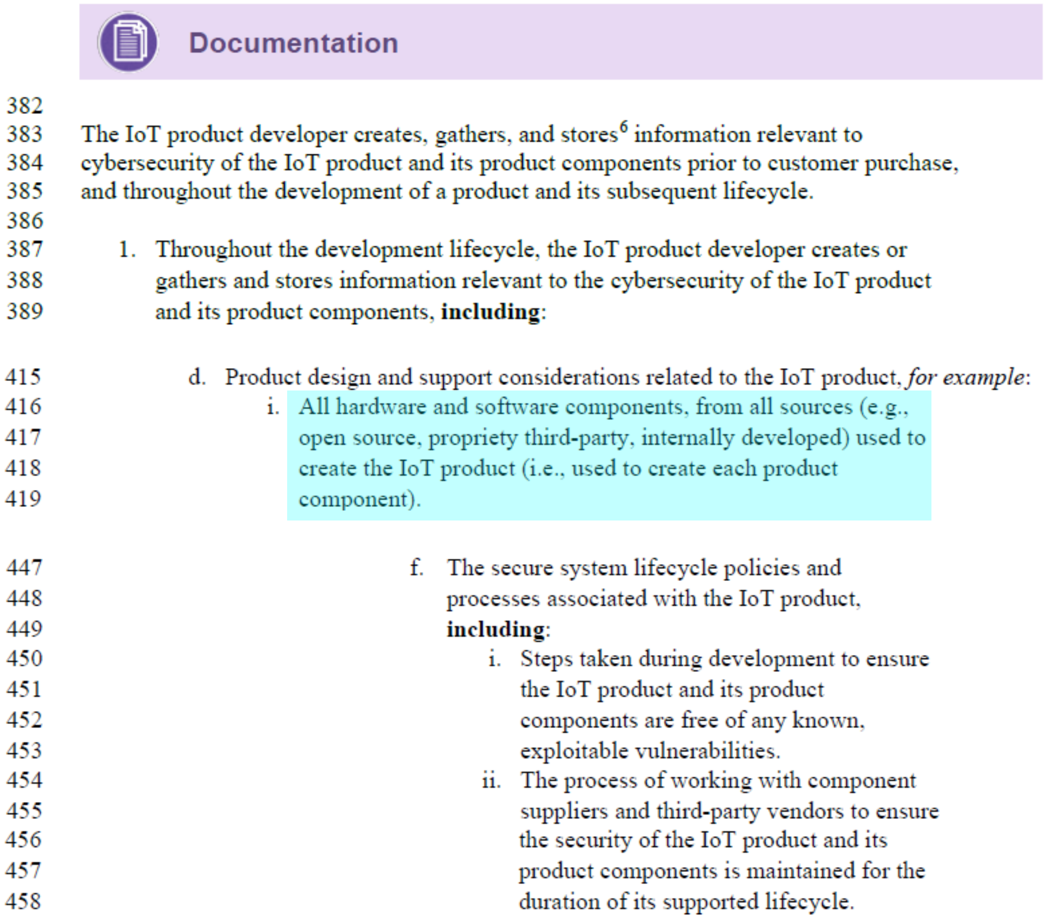
II.Policy

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;

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**:

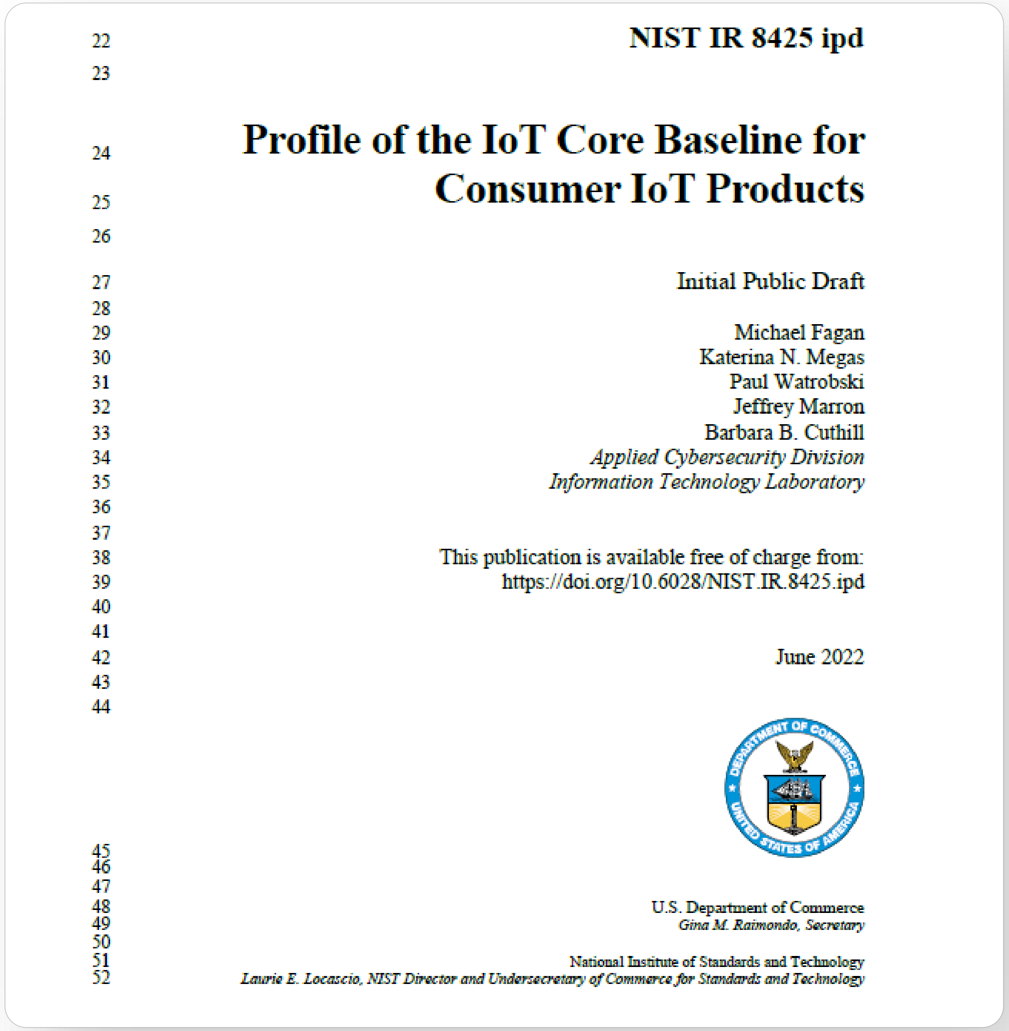
    d. Product design and support considerations related to the IoT product, *for example*:

    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

CENELEC Joint Technical Committee (JTC) 13 / Work Group (WG) 8

TIMELINE

- Jul 7, 2022 - JTC 13/WG8 established
- Feb 2, 2023 – First Draft (complete)
- Sep 2023 – Acceptance of Final Version
- Sep 2023 - Submission to Formal Vote
- Nov 2023 – Closure of Formal Vote
- Dec 2023 – Ratification and Availability of Definitive Text **

** Note – If 5G included then June 2024

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

- Access control mechanism –> access control of resources
- Authentication mechanism –> the entity is what it claims to be
- Update mechanism –> patch vulnerabilities
- Secure storage mechanism –> privileged data at rest
- Secure communication mechanism –> privileged data in motion
- Logging mechanism -> events that might impact privileged data
- Deletion mechanism -> deletion of privileged data
- Resilience mechanism -> mitigate DOS attack and return to defined state after attack
- Attack surface reduction -> input validation
- Network monitoring mechanism -> detect DOS and defend
- Traffic control mechanism -> source address validation
- User notification mechanism -> notify user of changes of privileged data
- Critical Security Parameter (CSP) generation mechanism -> i.e. strong passwords, crypto keys, etc.
- General equipment capabilities – up-to-date software and hardware with no known "exploitable" vulnerabilities, no unnecessary external interfaces,
- Cryptography -> shall use for Secure Update, Secure Storage, Secure Comms, CSP generation, etc.

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 Software Development Lifecycles (Secure SDLC) which include public product incident response programs for a continuous feedback loop
    - Software Bill of Materials (SBOM)

works with
BY SILICON LABS

Q&A