NEURONIC WORKS

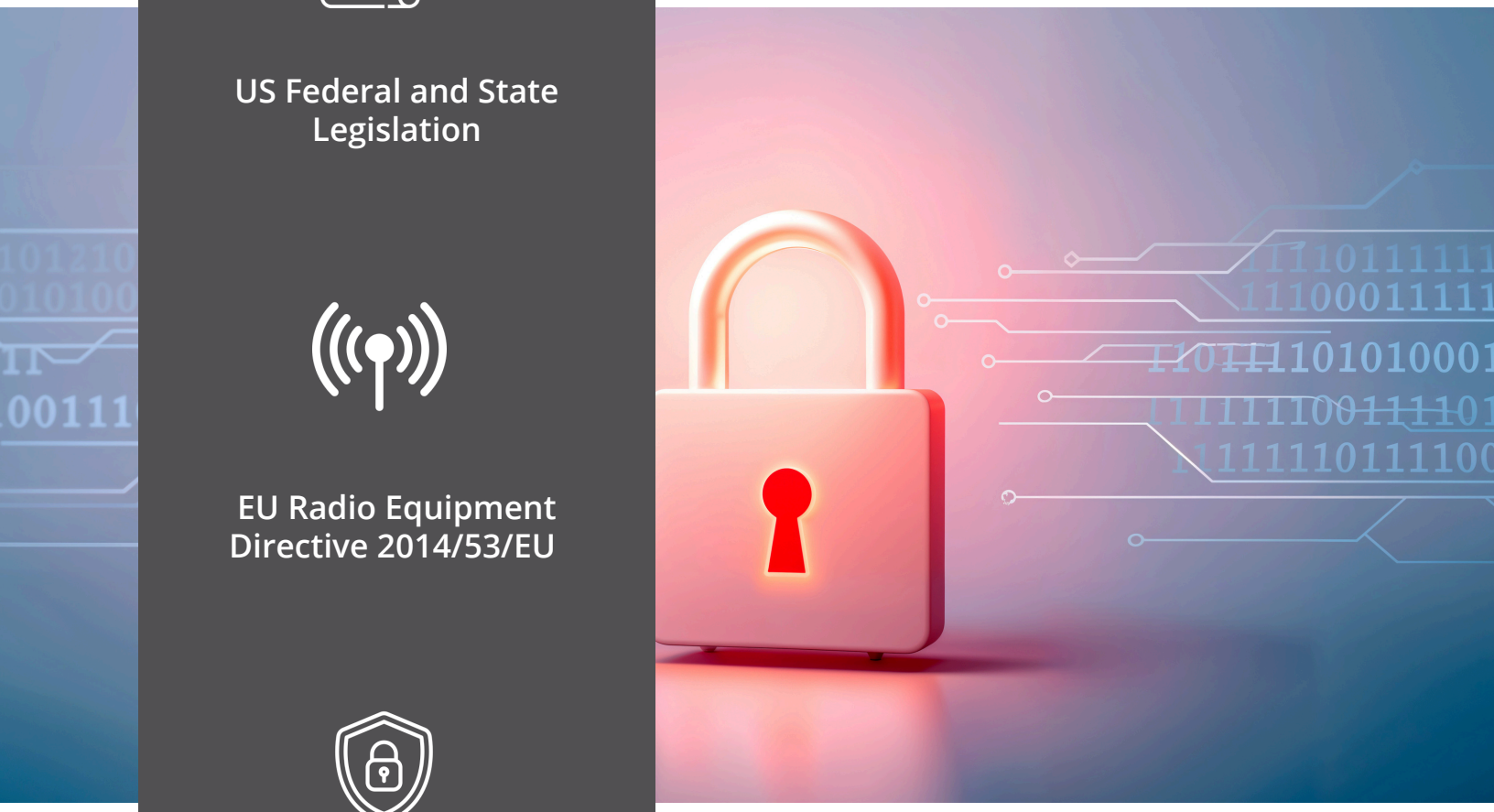
CYBERSECURITY REGULATIONS FOR CONSUMER IOT DEVICES

LEARN ABOUT

US Federal and State Legislation

EU Radio Equipment Directive 2014/53/EU

Singapore Cyber Trust Mark Labeling scheme



INTRODUCTION

Bringing your commercial or consumer IoT Devices with direct or indirect wired and/or wireless access to the Internet to various world markets entails that the device be professionally designed, verified, validated. Per each country's legislation, the IoT Device must be certified by the country's assigned Cyber Security Agency via accredited laboratories. This will ensure that all personal data, network ID and/or financial confidential data through local or cloud-based intermediate equipment is protected from hacking, attacks (by Software or Hardware), theft or misuse.

This document will present the various existing laws, regulations and directives in various jurisdictions, their requirements, and the stated guidance documents or standards used for:

1. US Federal and State legislation
2. EU Radio Equipment Directive 2014/53/EU and
3. Singapore Cyber Trust Mark Labeling scheme

NEURONIC WORKS

DEFINITIONS

a. IoT Device:

Consumer or commercial digital hardware and embedded firmware device incorporating one or more wired or wireless radio transmitter, receiver and/or transceiver with one or more antennas.

b. IoT Product:

An IoT device or device and any additional product components (e.g., back end, mobile device application) that are necessary to use the IoT device beyond basic operational features.

c. IoT Product Component:

Other kinds of equipment, multiple backends or companion components. Examples include:

i. Specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used).

ii. Backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device).

iii. Companion application software (e.g., a mobile app for communicating with the IoT device).

NEURONIC WORKS

CURRENT WORLDWIDE LAWS AND REGULATIONS

I. USA (State-level):

As of October 2024, there are two official state laws and one FCC Regulation covering Cybersecurity of IoT devices and Wireless/wired radio products with Internet access in the USA:

i. California US SB-327:2018 (IoT security law for all IoT devices as of January 2020)
ii. Oregon HB 2395:2023 (IoT security law for consumer IoT devices only)

Key points of the above State Laws:

1. The California law states: all IoT devices need unique passwords
2. The requirement for “reasonable security” is not clear because it is not defined
3. The California law applies to all IoT devices; Oregon’s law only applies to consumer IoT
4. Stores, marketplaces, or others selling IoT devices are not liable
5. The law does not apply if a user installs software from other companies
6. The law is not a reason to prevent the user from being able to modify the device
7. It doesn’t apply over federal laws or to businesses subject to HIPAA

II. USA (Federal-level):

The 'U.S. Government Cyber Trust Mark' (per FCC Title 47/Chapter I/Subchapter A/Part 8: SAFEGUARDING AND SECURING THE INTERNET):
This is a voluntary cybersecurity labeling program for internet-connected smart devices designed to give consumers the tools needed to make informed decisions regarding security, when purchasing consumer IoT devices (e.g. Voice-activated devices, Smart Lighting systems, Robot Vacuum cleaners, Wireless broadband routers, Smart thermostats, Smart appliances, Smart televisions, Baby Monitors, Connected Security systems, etc.), to bring into their homes. FCC has designated UL Solutions as the Lead Administrator. The FCC has so far announced ten designated CLAs (Cyber Trust Label Administrators) to certify consumer IoT devices (FCC Announces 10 Administrators of IoT Labeling Program | Federal Communications Commission). The FCC will announce very soon the accredited ISO/IEC 17025:2017 CyberLABs to assess and test consumer IoT products for compliance.

NOTES:

1. The above California & Oregon state laws show that the conformity assessment criteria is the NIST IR 8259A (NIST cybersecurity baseline for IoT devices) criteria document.
2. For IoT Devices with hardware and embedded software (firmware), the NIST CSWP 33 ipd (Product Development Cybersecurity Handbook Concepts and Considerations for IoT Product Manufacturers) Initial Product Draft is a practical application document based on NIST IR 8529. It is available at this website: Product Development Cybersecurity Handbook: Concepts and Considerations for IoT Product Manufacturers

3. The FCC U.S. Cyber Trust mark Labeling 'Fact Sheet' (Report and PS docket # 23-239) shows that the technical conformity assessment criteria will be the NIST IR 8425 (NIST Profile of the IoT Core Baseline for Consumer IoT Product) document. UL Solutions has not identified standards or testing procedures as of Jan. 2025. A detailed explanation of the U.S. Cyber Trust Mark from the FCC is available at this website: U.S. Cyber Trust Mark | Federal Communications Commission

4. The FCC US Cyber Trust Mark Label program states that certain IoT consumer product manufacturers and entities are prohibited from obtaining the use of the Label; these include:

i. All communications equipment on the FCC Covered List
ii. IoT devices or IoT products produced by any entity, affiliates or subsidiaries identified on the Department of Commerce's Entity List
iii. IoT devices or IoT products produced by any entity, affiliates or subsidiaries identified on the Department of Defense's List of Chinese Military Companies
iv. IoT products produced by entities owned, controlled, or affiliated with individuals or organizations that have been suspended or debarred from federal procurements or financial awards
v. IoT products produced by entities that are listed as ineligible for awards in the General Services Administration's System for Award Management

III. European Union:

EU Delegated Regulation 2023/2444, EU Delegated Regulation 2022/30 address the essential security requirements of EU Radio Equipment Directive (RED) 2014/53/EU Articles 3.3(d), 3.3(3) and 3.3(f). These cyber security testing/assessment requirements apply to most consumer and most commercial IoT Devices with one or more wireless radio transmitters/transceivers; this is required for consumer/commercial wireless and wearable products as of Aug. 1, 2025. Reference CENELEC standards are below; these standards are now harmonized in the EU Official Journal as of Jan. 31, 2025.

1. EN 18031-1 (Part 1: Internet-connected radio equipment)
2. EN 18031-2 (Part 2: Radio equipment processing data, internet-connected radio equipment, childcare radio equipment, toys radio and wearable radio equipment)
3. EN 18031-3 (Internet-connected radio equipment processing virtual money or monetary value)

NOTES:

As of March 2023, all IoT device compliance can be done via the following RED Directive Conformity schemes:

1. Module A (Internal Production Control with technical documentation) via the above EN 18031-x harmonized standards. At this time, only European-based certification bodies are accredited to 2014/53/EU Articles 3.3(d), 3.3(3) and 3.3(f).
2. Module B (EU Type Examination certification by an EU Notified Body) and Module C (Conformity to type based on Internal Production Control).

    i. The EU Cyber Resilience Act 2024/2847(CRA) states the cyber security requirements for ALL commercial and consumer devices with digital elements (with OR without radio modules) must be compliant to all applicable directive requirements to be placed on the EU Market as of December 11, 2027.

IV. Singapore:

Cyber Security Agency (CSA) Cyber Trust Mark for IoT devices, which requires the CSA Cybersecurity Labeling Scheme (CLS) certification: voluntary cybersecurity labelling scheme for consumer smart devices. Reference standards are:

i. ISO/IEC 15408 (Common Criteria for IT Security Evaluation)
ii. ETSI EN 303 645 (Cybersecurity for Consumer IoT: Baseline Requirements).

NOTES:

Under the CLS(IoT) scheme, smart devices will be rated according to their levels of cybersecurity provisions. This will enable consumers to identify products with better cybersecurity provisions and make informed decisions.

The CLS(IoT) was first introduced to cover Wi-Fi routers and smart home hubs. These products were prioritized because of their wider usage, as well as the impact that a compromise of the products could have on users. It has since been extended to include many consumer IoT devices, such as IP cameras, smart door locks, lights and printers. The CSA cybersecurity Certification Centre supervises the evaluation of the Sponsor/Developer product from an ISO 17025:2017 accredited Common Criteria Testing Laboratories (CCTLs) per the Singapore Common Criteria Scheme (SCCS) and the National IT Evaluation Scheme (NITES). List of current approved Laboratories: SCCS and NITES Approved Laboratories | Cyber Security Agency of Singapore

V. Industry:

Connectivity Standards Alliance (CSA) Consortium for Smart Home devices. Reference standards are:

i. ISO/IEC 15408 (Common Criteria for IT Security Evaluation)
ii. ETSI EN 303 645 (Cybersecurity for Consumer IoT: Baseline Requirements)
iii. NIST IR 8425 (NIST Profile of the IoT Core Baseline for Consumer IoT Product)

NEURONIC WORKS

US CYBER TRUST MARK REQUIREMENTS

The following sections are excerpts applicable to commercial/consumer IoT devices from FCC Fact Sheet FCC-CIRC2403-01 and NIST 8425.

1. IoT Product Technical Capability criteria

a) Device Identification:

The product can be uniquely identified by the customer and other authorized entities and the product uniquely identifies each IoT product component and maintains an up-to-date inventory of connected product components.

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

b) Device Configuration:

The configuration of the IoT product is changeable, with an ability to restore a secure default setting, and changes can only be performed by authorized individuals, services, and other IoT product components.

i. Cybersecurity Utility: The ability to change aspects of how the IoT product functions can help customers tailor the IoT product's functionality to their needs and goals. Customers can configure their IoT products to avoid specific threats and risks they know about based on their risk appetite.

c) Data Protection:

The IoT product protects data stored across all IoT product components and is transmitted both between IoT product components and outside the IoT product from unauthorized access, disclosure, and modification.

i. Cybersecurity Utility: Maintaining confidentiality, integrity, and availability of data is foundational to cybersecurity for IoT products. Customers will expect that the data is protected and that the protection of data helps to ensure safe and intended functionality of the IoT product. This means no common hard-wired passwords and no fixed IP addresses for uploading to cloud server database applications.

d) Logical Access to Interfaces Control:

The IoT product restricts logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.

i. Cybersecurity Utility: Enumerating and controlling access to all internal and external interfaces to the IoT product will help preserve the confidentiality, integrity, and availability of the IoT product, its components, and data by helping prevent unauthorized access and modification.

e) Software Update:

The software of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.

i. Cybersecurity Utility: Software may have vulnerabilities discovered after the IoT product has been deployed; software update capabilities can help ensure secure delivery of security patches.

f) Cybersecurity State Awareness:

The IoT product supports the detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

i. Cybersecurity Utility: Protection of data and ensuring proper functionality can be supported by the ability to alert the customer when the device starts.

2. IoT Product Developer Activities/Non-Technical Supporting Capability criteria

For this criteria, the IoT product developer creates, gathers, and stores information relevant to the cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.

a) Documentation:

The IoT product developer creates, gathers, and stores 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.

i. Cybersecurity Utility: Generating, capturing, and storing important information about the IoT product and its development (e.g., assessment of the IoT product and development practices used to create and maintain it) can help inform the IoT product developer about the product's actual cybersecurity posture.

b) Information and Query Reception:

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

i. Cybersecurity Utility: As IoT products are used by customers, those customers may have questions or reports of issues that can help improve the cybersecurity of the IoT product over time.

c) Information Dissemination:

The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.

i. Cybersecurity Utility: As the IoT product, its components, threats, and mitigations change, customers will need to be informed about how to securely use the IoT product.

d) Product Education and Awareness:

The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.

i. Cybersecurity Utility: Customers will need to be informed about how to securely use the device to lead to the best cybersecurity outcomes for the customers and the consumer IoT product marketplace.

With evolving laws and standards across jurisdictions such as the U.S., the EU, and Singapore, compliance with cybersecurity regulations is no longer optional but a critical requirement for market entry and consumer trust.

Moving forward, global cybersecurity regulations will likely continue to evolve, requiring continuous adaptation from IoT developers and policymakers. By prioritizing cybersecurity from the design phase to market deployment, companies can mitigate risks, protect user data, and contribute to a more secure and resilient digital world.

To book a free consultation with an experienced member of our Regulatory Standards and Certifications team, reach out to NeuronicWorks at info@neuronicworks.com

NEURONIC WORKS

NeuronicWorks Inc.
210 Lesmill Rd
North York, ON
M3B 2T5
+1 844-546-1575

info@neuronicworks.com
www.neuronicworks.com