Compliance & Risks

Cybersecurity Certification Requirements for Connected Products - Global Developments

Author: Aaron Green, Ph.D
Senior Regulatory Compliance Consultant, Compliance & Risks

4 April, 2023

Further regulatory developments may have occurred after publication. To keep up-to-date with the latest compliance news, [sign up to our newsletter]

About The Author

Aaron Green
Senior Regulatory Compliance Consultant,
Compliance & Risks

Dr. Aaron Green, J.D., P.hD., is a senior regulatory compliance consultant who has been with Compliance & Risks since 2008.

His areas of expertise include wireless/connectivity, electromagnetic compatibility, and automotive regulations.

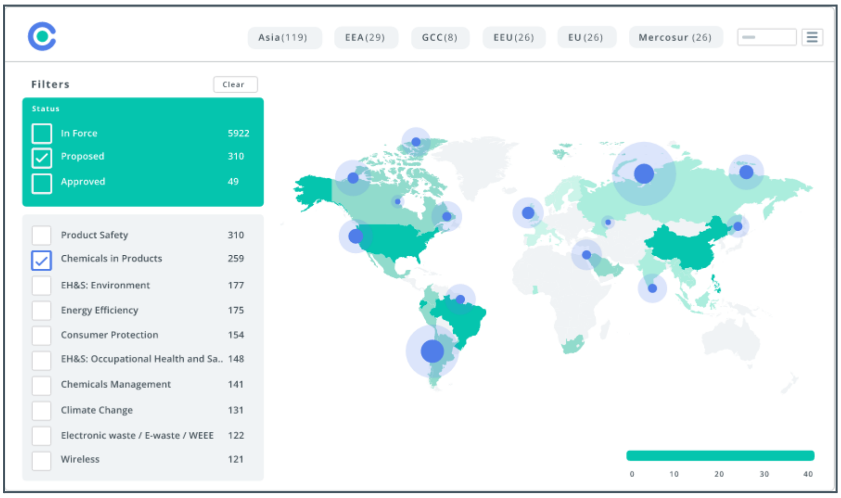
He received his juris doctor from the University of Wisconsin and his Ph.D. from T.U. Dublin. Prior to joining C&R, he practiced law in Minnesota (USA).

Unlocking Market Access

At Compliance & Risks, we help you keep on top of global regulatory changes and their impact worldwide. We have the right technology, regulatory content and expertise to help you unlock market access, protect revenue and elevate the role of compliance.

Our Solution includes:

- C2P: The most advanced product compliance software on the market, helping you streamline your compliance process and unlock market access around the world.
- Regulatory Content: We provide the broadest and most comprehensive product compliance regulatory content on the market, monitoring 195+ countries, 20 industry sectors, 41+ topics and 70,000+ regulatory sources.
- Ask our Experts: Direct access to our team of experts for support



Filters

Status

□	In Force	5922
☑	Proposed	310
□	Approved	49
□	Product Safety	310
☑	Chemicals in Products	259
□	EH&S: Environment	177
□	Energy Efficiency	175
□	Consumer Protection	154
□	EH&S: Occupational Health and Sa..	148
□	Chemicals Management	141
□	Climate Change	131
□	Electronic waste / E-waste / WEEE	122
□	Wireless	121

Additionally, we offer:

- Market Access Services: Our Market Access team helps you understand your product compliance obligations by transforming regulations into actionable knowledge with tailored advice for you and your business.

Why choose C2P?

- Stay ahead of regulatory changes with the world's most comprehensive regulatory database
- Avoid delays with alerts of changes to regulations & requirements in real time
- Improve efficiency with powerful collaboration and workflow tools to keep compliance evidence up-to-date & live linked back to Regulations, Standards & Requirements

Contact us to speak to one of our team today to learn how you can simplify your regulatory compliance process.

For more information, please visit www.complianceandrisks.com

Important Notice: All information provided by Compliance & Risks Limited and its contributing researchers in this report is provided for strategic and informational purposes only and should not be construed as company-specific legal compliance advice or counsel. Compliance & Risks Limited makes no representation whatsoever about the suitability of the information and services contained herein for resolving any question of law. Compliance & Risks Limited does not provide any legal services.

1. Introduction

Recently, one of my colleagues was asked to explain what an oxymoron was, and the only example he could think of was cybersecurity.
This raises two important points that I hope to touch on here.

Firstly, regulatory consultants are thinking about cybersecurity a lot; and secondly, there is an inherent conflict between connectivity and security. The conflict within the idea of cybersecurity arises from the fact that cyberspace exists for sharing information, but security demands that access is restricted. What this means, in practice, is that cybersecurity is one part technical and nine parts social.

For example, in the wake of the NotPetya worm that disabled all IT systems at the global shipping company Mearsk, the company continued operating through human ingenuity as automated online bookings were replaced by private WhatsApp messages and standard shipping labels were replaced by hand-written post-it notes.

Ultimately, the company's software systems were recovered from a server in a remote port town that had been offline during the infection due to a power outage in the region. The vital data was then hand-delivered to Mearsk headquarters in Denmark because the local internet connection was so slow that it would have taken longer to transfer the data over the internet.

This episode underlines the fact that security is a function of inaccessibility, which means that cybersecurity requirements are by definition both too onerous and too lax. Nevertheless, there is a set of emerging regulations, international standards and best practices that attempt to find a balanced approach to cybersecurity.

Globally, there is a growing interest in establishing basic cybersecurity requirements for connected and connectable digital devices.

The following section outlines a selection of the most significant recent developments.

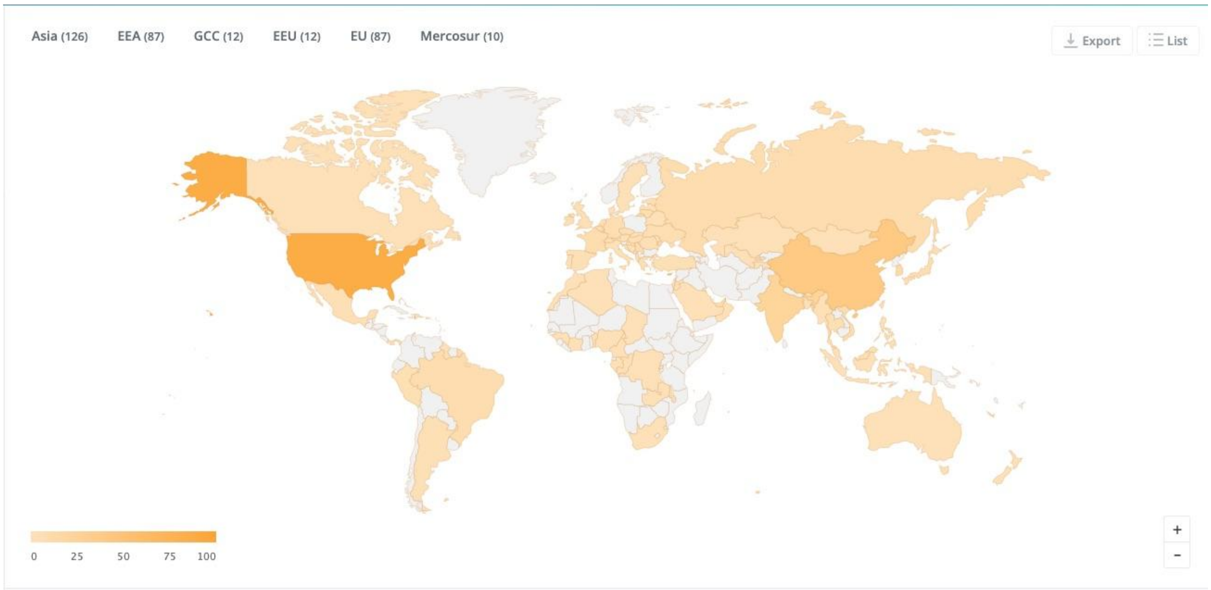


Figure 1. Heat Map of Cybersecurity Regulations
(Source: C2P By Compliance & Risks)

2. National and Regional Regulations

European Union

In October 2022, the European Union published delegated regulation (EU) 2022/30 to require cybersecurity protection for radio equipment under the Radio Equipment Directive. Radio equipment will need to be certified as compliant with the essential requirements related to cybersecurity from 1 August 2024.

The EU has issued a request to CENELEC to draft a harmonised standard in support of the essential requirement set out in Article 3(3), point (d/e/f), of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30. According to the EU request, the forthcoming harmonised standard should contain technical specifications for the following capabilities:

1. monitor and control network traffic, including the transmission of outgoing data;
2. mitigate the effects of ongoing denial of service attacks;
3. authentication and access control mechanisms;
4. on a risk basis, up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities;
5. automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities;
6. protect the exposed attack surfaces and minimise the impact of successful attacks.
7. protect stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access, disclosure, unauthorised destruction, loss or alteration or lack of availability;
8. include functionalities to inform the user of changes that may affect data protection and privacy;
9. log the internal activity that can have an impact on security; and
10. allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information;

It should be noted that these requirements are similar to the requirements in the existing ETSI standard (EN) 303 645 for consumer IoT devices, outlined below.

In requesting a new standard, the EU seeks to integrate insights that have emerged since the implementation of the existing standards and apply them broadly to all radio equipment.

In addition to the cybersecurity requirements for radio equipment, the EU has also proposed a cybersecurity law applicable to all equipment "with digital elements" that could be subject to cyber attack, called the Cyber Resilience Act.

Equipment with digital elements is defined broadly to include any device that can download or upload digital information, whether through direct contact or wirelessly.

This draft law sets out four specific objectives:

1. ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;
2. ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
3. enhance the transparency of security properties of products with digital elements, and
4. enable businesses and consumers to use products with digital elements securely.

The proposed requirements for equipment with digital elements mirror those envisioned for radio equipment, so it is envisaged that the standardisation work carried out in the context of the RED will be taken into account to facilitate the implementation of this regulation.

Brazil

One of the first pieces of legislation dedicated to cybersecurity for internet-connected devices was Brazil's Act No. 77 of 2021. This law establishes basic cybersecurity requirements for connected devices subject to type approval, including secure software installation and updates, remote management, secure communications, unique passwords and appropriate encryption for the transmission of passwords, access keys and credentials.

The law may be satisfied by a declaration of conformity with suitable international standards (e.g., ETSI EN 303 645, ISO/IEC 27402).

Brazil is also one of a growing number of jurisdictions enacting specific cybersecurity requirements for customer network modems and routers. On 7 March 2023, ANATEL published Act No. 2436, which will enter into force on 10 March 2024.

This Act establishes minimum cybersecurity requirements of mandatory application for conformity assessment of the following customer premise equipment (CPE) employed to connect subscribers to the Internet service provider's network:

- Cable modem;
- xDSL modem;
- ONU, ONT;
- Router or modem intended for fixed wireless access (FWA - Fixed Wireless Access);
- Router or modem intended for fixed broadband access via satellite;
- Wireless router or access point.

The Act addresses requirements for factory-supplied passwords, user-defined passwords and the prevention, detection and reporting of vulnerabilities in CPE.

India

India’s Telecommunications Engineering Centre (TEC) has introduced a range of security assurance standards, called Indian Telecom Security Assurance Requirements, or ITSARs, that provide guidelines for the security of information products. ITSARs have been released for network equipment and end-point user equipment.

On 2 February 2023, the TEC announced that conformity with the relevant ITSAR will be required for WiFi CPE and IP Router equipment for applications submitted on the MTCTE certification portal starting on 1 July 2023.

The specific elements of the ITSARs for Router and WiFi equipment reflect the general consensus on cybersecurity requirements for network equipment:

- Access and Authorization (usage of cryptographically protected network protocols)
- Authentication Attribute Management (strong password, inactive session timeout)
- Software Security
- System Secure Execution Environment (Unused functions deactivated)
- User Information Audit (log all important Security events)
- Data Protection (Cryptographic Based Secure Communication)
- Network Services (filter incoming IP packets on any IP interface)
- Attack Prevention Mechanisms (measures to deal with overload situations)
- Vulnerability Testing Requirements (only documented ports respond to outside requests)
- Operating System (dynamic content (log files, uploads, etc. shall not influence system functions)

China

China has released guidelines for the development of cybersecurity standards for IoT devices.

The basic security standard system for the internet of things includes overall security, terminal security, gateway security, platform security and security management standards.
The plan calls for terminal security standards to have been completed in 2022, but they have not yet been released.

3. International Standards

ETSI (European Telecommunications Standards Institute)

ETSI (EN) 303 645 V2.1.1 (2020-06): Cyber Security for Consumer Internet of Things: Baseline Requirements:
This standard provides specific requirements for consumer devices under the following headings:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Critical security parameters should be encrypted in transit
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Resilience should be built into consumer IoT devices and services, taking into account the possibility of outages of data networks and power.

ISO/IEC

ISO/IEC 27402 Cybersecurity — IoT security and privacy — Device baseline requirements:
This document provides a baseline set of ICT requirements so that IoT devices are able to support security and privacy controls. A risk assessment is needed to develop a risk treatment plan that identifies the necessary features and countermeasures to implement.
Management of systems using IoT devices depends (in part) upon the capabilities of those devices.

Broadly speaking, this document addresses ICT requirements for IoT devices that are made available to the market.

This document is intended as a baseline, upon which vertical markets (such as health, financial services, industrial, consumer electronics and transportation) can build additional requirements for the expected use and risks of IoT devices in their applications. In addition to this document, various sectors (e.g. private/industrial, public, defence, national security) and vertical markets have sector- or vertical-specific standards, for example EN 303 645 for consumer devices and the IEC 62443 series for industrial devices and systems.

While this document can provide requirements for a conformity assessment scheme, it is expected that stakeholders for specific sectors and vertical markets will develop consensus around requirements specific to their contexts, building "on top" of this baseline standard.
Subsequently, conformity assessment programs can be developed around those specific sectors and vertical markets, and this document would be effectively integrated into such programs while providing a common set of baseline requirements.

4. Conclusion

The paradox of cybersecurity means that the legislative environment is one of constant tension and flux. Security that is adequate today may be obsolete tomorrow, so all present and future cybersecurity requirements must incorporate the state of the art as it will evolve into the future.

According to the GSMA IoT cybersecurity guidelines:

For the Internet of Things to evolve effectively, we must resolve the security challenges inherent to its growth.
These challenges are:

- Availability: Ensuring constant connectivity between Endpoints and their respective services
- Identity: Authenticating Endpoints, services, and the customer or end-user operating the Endpoint
- Privacy: Reducing the potential for harm to individual end-users
- Security: Ensuring that system integrity can be verified, tracked, and monitored

Addressing these issues in real time will require the coordination of efforts across all sectors engaged in delivering IoT equipment and services, as well as continuous engagement with regulatory authorities.

No specification can answer the question how secure is secure enough?

This is a political question, not a technical one, so the answer will shift with the environment through updates and interpretations to the law.