MARCH 2024

Securing IoT Devices for Consumers

TIC Council Recommendations

TIC Council is the global trade association representing the independent TIC (Testing, Inspection and Certification) industry with over 100 members from leading Conformity Assessment Bodies (CABs) in 160 countries across the world. The TIC industry offers its services worldwide to ensure that only safe and secure consumer IoT products enter the market, to the benefit of consumers and the digital ecosystem worldwide.

+32 2 880 21 37 secretariat@tic-council.org www.tic-council.org

Summary

The concept of the Internet of Things (IoT) is evolving rapidly, with a growing number of connected devices flooding the market every day and everywhere. Daily, we encounter a wide variety of increasingly sophisticated, intelligent, and interconnected digital products through which people and businesses can make their homes and offices smart. These digital products are constantly communicating and sharing data with each other, creating a seamless but constant exchange of data and information. However, with all the data being collected, stored, and used by these devices, there is a long list of security risks for all IoT devices.

This raises the question of whether the rules currently in place on the market are still appropriate for dealing with these risks.

The aim of this paper is to present the various legislation and standards relating to connected devices in the European Union, the United States, China, and India and provide an in-depth analysis of the regulatory systems. The paper notes that, despite the cybersecurity mechanisms and tools currently available, cyberspace still lacks a coordinated and harmonised approach or the means to make current rules operational.

On page 11, you will find our recommendations for enhancing the security of IoT devices and legislation. These include creating global alignment between standards and certification processes, supporting the highest level of expertise among IoT workforces, establishing a consensus on baseline requirements for IoT security certification schemes, and promoting the involvement of third-party conformity assessment bodies along the value chain to reinforce Digital Trust.

Cybersecurity gap in the consumer IoT devices market

Internet of Things

"Global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."
Source: ISO/IEC 20924:2021

Consumer IoT devices

Consumer IoT devices are a heterogeneous range of connected devices. Consumer IoT devices possess embedded technologies (for example, processing chips, software, and/or sensors) that connect to the internet (via wired and wireless networks and various protocols) and collect and share data with each other and with users. Their specificity is to better serve end-users. They are often classified into:

Personal IoT devices include, connected toys, wearables, hearable, smartphones, or personal laptops (smart clothing, smart watch, smart glasses etc.).

Smart Home IoT devices include home appliances, home automation products like smart kitchen appliances and security systems with face recognition and voice control such as voice assistant, lighting fixtures, family entertainment etc.

The range of consumer IoT devices continues to expand with manufacturers gradually succeeding in seamlessly integrating IoT devices into a growing ecosystem of capabilities and uses. Today, consumer IoT devices enable us to support gaming and entertainment, or to provide health monitoring, home security, parental tracking, etc., thereby becoming an integral part of the way we interact with others in society.

In 2021, the global IoT market value exceeded $1 trillion, with the Asia-Pacific region in the leading position in the consumer technology market with a 42% sales share and 25% of sales coming from Europe. In the coming years, the consumer IoT market is expected to grow rapidly, with projections of 26.4 billion devices worldwide by 2026 and a global consumer IoT market size of $188 billion in 2027.

The challenges associated with consumer IoT devices

The growing use and circulation of consumer IoT devices offer significant opportunities for society and individuals. However, with this expansion comes a series of challenges that ultimately increase the complexity of cybersecurity on a global scale and pose concrete risks to individual lives as well.

A few examples illustrate the cybersecurity gap:

INTERNAL FACTORS

- The IoT devices attack surface is growing as they become more diverse, numerous and embedded, and ultimately more vulnerable to potential cyber-attacks.
- Connected devices are increasingly technologically complex and evolve regularly through updates and patches, making it difficult to secure them throughout their lifetime.

SYSTEMIC FACTORS

- The IoT space knows no boundaries and cyber incidents or attacks do not stop at physical borders.
- There are rogue operators who do not have cybersecurity objectives in mind and are currently placing low-cost and non-secure IoT devices on the market.
- Manufacturers, especially newcomers or Small and medium-sized enterprises (SMEs), do not always have the necessary cybersecurity expertise to implement the right processes to secure their products.

Two main types of threats usually arise from security breaches:

1. Firstly, a low level of cybersecurity can lead to **direct security and privacy risks**, including jeopardizing the confidentiality, integrity, and availability of data. While cybersecurity issues may affect individuals, they are a matter of great national or global concern.

- Cybersecurity breaches can lead to data theft, whether it is private photos on a laptop or confidential data in a company's server resulting in a loss of income or an inability to operate.
- The 2023 Cost of a Data Breach Report published by IBM Security revealed costlier and higher-impact data breaches than ever before, with the global average cost of a data breach reaching an all-time high of $4.35 million for studied organizations and increasing nearly 13% over the last two years of the report.

2. Secondly, and more surprisingly, a low level of cybersecurity can pose concrete threat to people's safety. Let's imagine that a cybersecurity incident affects the safety features of a device, making it materially unsafe. This is the case, for example, if a malicious cyberattack is launched on the safety feature of a lift, which disables the brakes and cause it to fall. While safety issues may mainly affect individuals on a limited scale, there is nevertheless the not-so-remote possibility that cyber-attackers can take control of IoT devices, escalate and target smart cities.

In any case, a cyber incident also leads to financial losses that can irrevocably shut down a company or nation's activity and cause a loss of trust in the company involved or the brand used. This can be the most damaging and insidious impact of cybercrime for companies victimized by hackers.

To address the safety and security risks arising from consumer IoT devices, harmonised minimum cybersecurity measures and protocols need to be implemented along the entire value chain, from device manufacture to end-user use.

Mapping of the current cybersecurity frameworks and related risks

While cybersecurity of consumer IoT products is a growing concern worldwide, legislators have decided to address IoT cybersecurity and privacy concerns in different ways. TIC Council relies on its regional branches to oversee the adoption of commercial and regulatory certification initiatives for consumer IoT cybersecurity that promote good practices and accelerate their deployment (see Annex I).

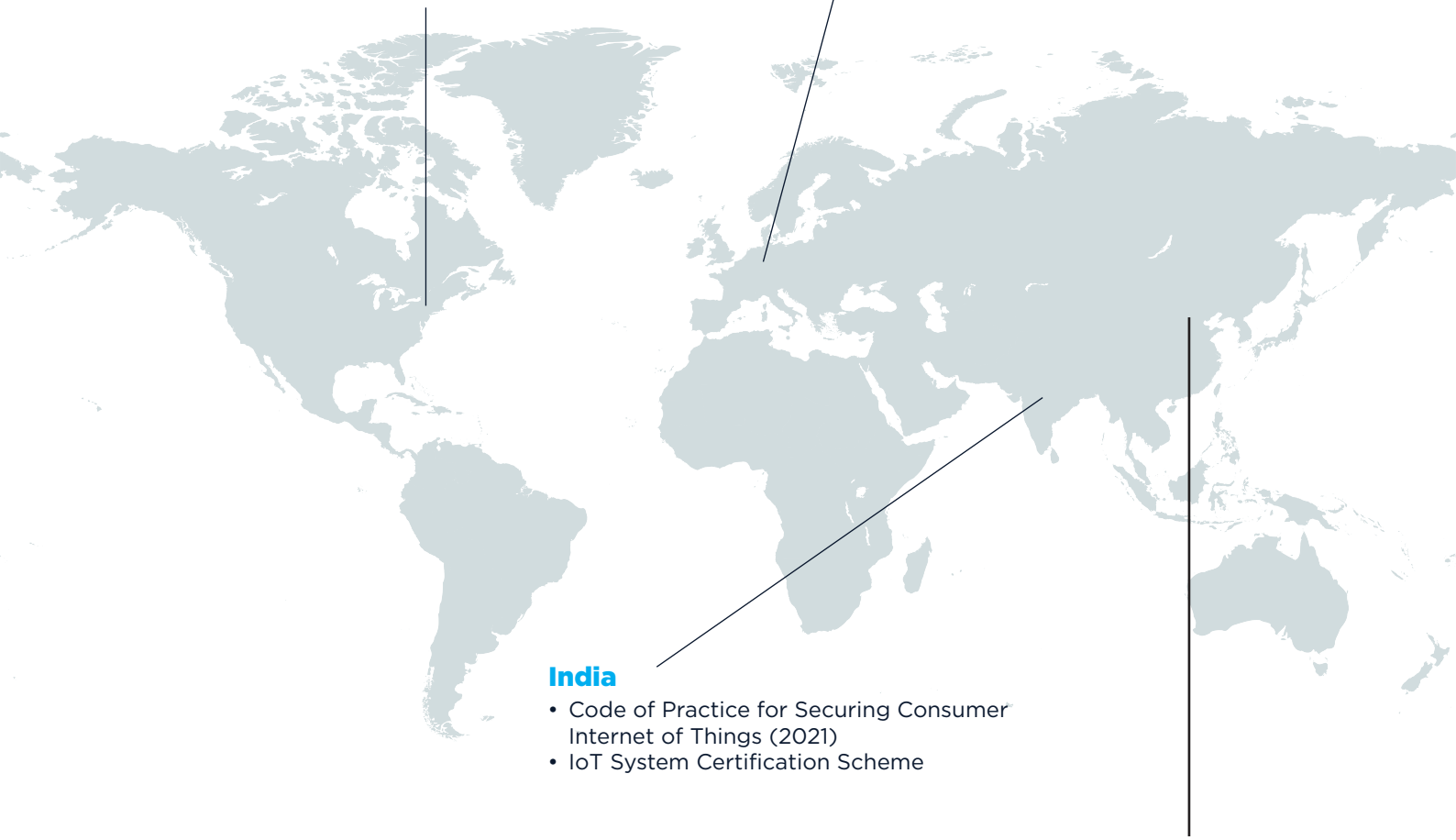
Disclaimer: The information below may change in line with new legislation.

European Union

- Cybersecurity Act (2019)
- Delegated Act of the Radio Equipment Directive (2022)
- Cyber Resilience Act (2022)

United States of America

- Cybersecurity Information Sharing Act (2016)
- Cybersecurity Framework (2018)
- Guidance on Securing IoT Devices (2020)
- Internet of Things Cybersecurity Improvement Act (2019)
- Executive Order on Improving the Nation's Cybersecurity (2021)



India

- Code of Practice for Securing Consumer Internet of Things (2021)
- IoT System Certification Scheme

China

- Cybersecurity Law (2016)
- General requirements for security operation and maintenance of IoT information System (2020)
- Data Security Law (2021)
- Personal Information Protection Law (2021)
- Notice on Printing and Distributing the Guidelines for the Construction of IoT Basic Security Standard System (2021)
- Three-Year Action Plan for the Construction of New IoT Infrastructure (2021-2023)

The United States of America

The cybersecurity of IoT devices became a legislative and political topic with the Cybersecurity Information Sharing Act (2016), and when the National Institute of Standards and Technology (NIST) issued the 2018 Cybersecurity Framework which is currently being updated. The growing importance of cybersecurity can be observed at different levels. As of 2020, the Internet of Things Cybersecurity Improvement Act is passed and requires the federal government to use certain security standards for IoT devices. The same year, the states California and Oregon adopted Bills adding security requirements for all IoT devices sold in these States. In 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released guidance on securing IoT devices, highlighting the unique cybersecurity challenges they pose. Finally, the Executive Order on Improving the Nation's Cybersecurity of May 2021 reinforces cybersecurity requirements for some of these devices. In addition to regulation, the United States relies on NIST guidance and on ISO/IEC standards such as IEC 62443-4-2 for international alignment.

Certification in this area is mainly used on a voluntary basis in the United States. The National Voluntary Laboratory Accreditation Program (NVLAP) accredits laboratories to perform testing. The Federal Trade Commission (FTC) is tasked with enforcing data privacy and security for consumer IoT products. Some private initiatives, such as the Cyber Threat Alliance (CTA), also aims to improve cybersecurity.

In conclusion, in the United States, there is nor a comprehensive national IoT cybersecurity regulatory framework, neither a comprehensive set of standards.

The European Union (EU)

The EU started implementing a comprehensive cybersecurity legislation package with the Cybersecurity Act (2019), which empowered European Union Agency for Cybersecurity (ENISA) and established an EU-wide certification framework as the preferred way to demonstrate compliance with cybersecurity rules. However, it was only in 2022 that the first mandatory cybersecurity requirements were adopted under the Delegated Act of the Radio Equipment Directive, which strengthens the cybersecurity of wireless devices. The same year, the European Commission proposed a Cyber Resilience Act which would impose harmonised cybersecurity requirements for all connected devices, including consumer IoT devices, throughout their lifecycle. From a standard perspective, European Standard Organisations are active in the cybersecurity field, with the release of ETSI EN 303 645, which has the potential to spread to other regions due to its comprehensive requirements and wide categories. The EU also applies ISO/IEC standards. It should also be mentioned that Member States perform market surveillance activities with their own budgets.

The EU's regulatory system is based on a precautionary approach following a risk-based principle, with different conformity assessment services mandated according to the risk that the product poses. Third-party conformity assessment bodies may be involved when products pose the greatest risks and may be designated as "Notified Bodies".

In summary, the EU is adopting an interventionist approach by which it appears as the regulatory region mandating essential requirements in the IoT world. Other regulatory initiatives are already on the way, such as the EU Cyber Solidarity Act and discussion about new certification schemes on IoT.

China

The IoT industry in China is developing rapidly, and the government attaches great importance to industry guidance and the cybersecurity and personal privacy protection in applications. This has led to the development of a trinity pattern of national industrial policies, regulations, and standards. Since 2016, the "Cybersecurity Law", "Data Security Law", "Personal Information Protection Law", and "General requirements for security operation and maintenance of IoT information System" have been introduced.

In addition, in 2019, China adopted the Information Security Technology - Basic Requirements for Network Security Level Protection also known as "Level 2 Protection", which mandates requirements on specific types of platforms, including cloud computing, mobile, IoT, industrial control systems, and big data. The Three-Year Action Plan for the Construction of New IoT Infrastructure (2021-2023) seeks to give full play to the important role of the IoT in promoting the development of the digital economy and enabling transformation. Besides, China has compiled a series of related technical standards in the IoT field. In 2021, the government released the Notice on Printing and Distributing the Guidelines for the Construction of IoT Basic Security Standard System (2021 Edition) to establish an IoT basic security standard system by 2022. However, the majority of standards come from industry initiatives, such as the "Technical Requirements for Smart Home Appliances with IoT Operating System" (T/CAS 520-527-2021) or "Technical Requirements for Smart Home Product Safety and Smart Door Lock Safety" (T/SETEA 000001-2019) launched by the Shanghai Electronic and Electrical Technology Association in 2019.

In China, compliance with cybersecurity rules is also based on the level of risk that a product poses. Independent Conformity Assessment Bodies could play a crucial role in ensuring that IoT products comply with cybersecurity regulations and standards for products above Level 2 since the government has established a national accreditation system for Conformity Assessment Bodies. Market surveillance activities are performed by authorities at the central and local levels to ensure the quality and safety of IoT products in the Chinese market.

Overall, China has made significant advances in developing its cybersecurity regulatory and standard environment in recent years by providing broad market prospects for the industry's development and creating a favourable production and operation environment for enterprises.

India

India's approach to cybersecurity emphasizes the importance of ensuring end-to-end security for connected IoT devices, with a second nested aim of protecting the privacy of individuals' personal data, particularly in the healthcare area.

To achieve this, India has implemented several measures and policies, including the Code of Practice for Securing Consumer Internet of Things (2021) mandating IoT devices to undergo mandatory testing and certification before they can be sold, imported, or used in India. This requirement helps to ensure that IoT devices meet certain security standards and are safe to use for individuals and organizations. The Code is aligned with the baseline requirements mentioned in ETSI EN 303 645. In 2023, a new IoT Regulation by the Telecom Engineering Centre (TEC) introduced new mandatory security testing for Wi-Fi CPE and IP Routers Products, demonstrating the emphasis put on the critical need for certification to mitigate the risk of uncertified equipment. In addition, India has established a National Trust Center (NTC) which serves as a platform where certified IoT devices are registered, and where any discovered vulnerabilities can be reported and addressed. This provides an additional layer of protection against potential cyber-

attacks. Finally, India has also established the IoT System Certification Scheme (IoTSCS), operated by the STQC Dte Ministry of Electronics and Information Technology, and designed to support all IoT systems and products.

In conclusion, India's approach to cybersecurity has already taken positive actions for ensuring the security of IoT devices and protecting individuals' personal data. The mandatory testing and certification requirements for IoT devices, as well as the establishment of the NTC and the IoTSCS, are crucial measures that help to ensure compliance with security standards and protect against potential cyber threats.

Analysis

Overall, it is clear that all four regions recognise the importance of IoT cybersecurity risks and have taken steps to address them. However, the differences in approaches taken and specific requirements highlight the challenges in achieving a globally harmonised approach to consumer IoT cybersecurity.

At present, there is no unitary global cybersecurity strategy.

- While the EU and US have adopted similar approaches by requiring a mandatory baseline security framework for IoT devices prior to sale, India and China have adopted voluntary approaches with the government playing a significant role in supporting regulations and standards. The significant differences in the specific requirements and approaches taken can make it challenging for companies operating in multiple regions to navigate and comply with the various regulations and standards. In addition, at present, not all regions incentivise uniformly the industry and especially IT manufacturers to put cybersecurity at the heart of their concerns, despite recent improvements.

- Most existing cybersecurity standards focus on specific sectors, use cases or regions which makes them effective in a limited framework. Harmonised global cybersecurity standards are yet to be truly developed and recognised. In all regions, standards are yet to be developed to take account of the specific nature of IoT devices. The first globally applicable standard ETSI EN 303 645 is already a step in the right direction and is already the basis for many organisations' products and international private certification schemes. However, as standardisation processes may take longer than expected collaboration between government, private sector, academia, and civil society is essential to promote a shared responsibility for cybersecurity.

- The involvement of CABs in the design and development phases of connected devices is still disparate across regions. The European Union is the only region where the TIC industry would be involved both mandatorily (with the forthcoming Cyber Resilience Act) and voluntarily (with the Cybersecurity Act) to verify the compliance of IoT devices with EU regulations before being placed on the market. This would at least be the case when devices are presented as carrying a high risk to the individual or society, or when specific sectors are concerned, such as critical national entities. In other regions, regulatory systems do not foresee the mandatory involvement of CABs, but they can be involved upon the manufacturer's choice. Those divergences do not facilitate the manufacturer's understanding of cybersecurity issues or the global level playing field for IT manufacturers.

The TIC sector: a crucial actor to make the consumer IoT world more secure

The independent TIC sector provides conformity assessment services to protect people and the environment, ensuring that an object of conformity assessment meets the requirements in a specified standard. Given the lack of maturity of the IoT devices market from a cybersecurity perspective, the TIC industry should verify the compliance of a large number of consumer IoT devices to increase their safety and security for end users and manufacturers.

The independent TIC sector in the cybersecurity space

The TIC industry caters to various industry sectors worldwide from consumer products, medical devices, petroleum, mining to food and agriculture among others. In the cybersecurity and IoT area, TIC companies provide technical expertise ensuring the safe operation and security of IoT devices (see Annex III).

Disruptive technology: the TIC sector supports the development and safe adoption of innovative technologies, including artificial intelligence, autonomous transport, and connected devices.

Privacy and security: TIC services also ensure the confidentiality and security of personal and commercial data handled by telecommunications providers and users, meeting national standards for security equipment, and facilitating the use of biometric identification.

In practice, a Conformity Assessment is the demonstration that a product, service, system, process, installation, claim, person, body, etc., (or "object of conformity assessment") meets requirements. These requirements may be in a regulation or a standard or other normative document.

Conformity assessment may be performed by different players in the manufacturing chain but most generally by the manufacturer itself or a third independent entity (see Annex II).

The TIC sector is a major contributor to the global economy and quality of daily life around the world: we provide the guarantee that products are safe, secure, effective, reliable, of quality, and sustainable.

In addition, the TIC industry is part of a wider ecosystem known as the 'Quality Infrastrutre (QI) ecosystem', which brings together Standards Bodies, Conformity Assessment Bodies and Accreditation Bodies to control quality and ensure the safe of people and society. Through its approach based on common standards, conformity assessment and accreditation programs, the QI ecosystem enables the efficient operation of domestic markets and access to foreign markets.

With the rise of new digitalisation challenges, such as the cybersecurity of connected devices, the cybersecurity community and policymakers should use the QI ecosystem to place compliant and secure prodyctcs on the market.

In order to support the safety and security of consumer IoT products, the involvement of the TIC industry and the Quality Infrastructure ecosystem in the compliance mechanisms of forthcoming cybersecurity legislations should be seen positively by security players, even when harmonised standards are available.

TIC Council recommendations for a secure IoT future

TIC Council members, with their key position between the industry, policymakers, and standard organisations, are ready to provide their services to support the safe operation and security of connected devices. Further, we suggest following these recommendations:

1. Creating global alignment between standards and certification processes

The numerous existing certifications and standards for cybersecurity have created confusion in the market, slowing down market acceptance, and preventing the creation of an industry-wide standard. It is therefore necessary to create a consensus in the specification of requirements for certifying cybersecurity of IoT devices.

TIC companies operate worldwide and provides conformity assessment services in different markets and sectors. This rare position makes them the pivotal player with a profound comparative understanding of regional frameworks. This allows the TIC sector to work with policymakers, the industry, standard organisations, and consumers simultaneously thanks to its wide state-of-the-art expertise and to disseminate the best practices efficiently.

The TIC sector is a legitimate/relevant player to advise on the various cybersecurity schemes, processes and standards that should be used globally and create recommendations and guidelines for how various types of requirements can be met. Thanks to its global expertise, the TIC industry can create a level playing field with higher levels of regulatory compliance, cost savings and potential creation of market shares.

2. Supporting the highest level of expertise of the IoT workforces

The IoT market is flooded with a wide variety of players of varying sizes, resources, and cybersecurity expertise. It is necessary to ensure that a consistent and superior quality of service is provided by all cybersecurity players during the design, development, and testing of IoT products.

The TIC sector has succeeded in building a competitive ecosystem whose staff have extensive skills in meeting cybersecurity testing and certification requirements, updated by in-house training to ensure that their level of qualification reflects the latest state of the art. What's more, it already has all the necessary equipment for testing and certification, enabling processes to be optimised and for the compliance costs to be reduced.

The TIC sector is a reliable partner which has the required cybersecurity and legislation expertise to support the uptake of IoT principles in the cybersecurity community. The TIC industry, as a player already with a trained workforce, could assist cyber players to equip themselves properly. However, the development of harmonised evaluator's competencies accredited schemes would bring an even higher level of assurance to the industry, increased confidence in the quality and consistency of the services offered, and a level playing field for existing CABs by harmonizing market access conditions.

3. Create a consensus on baseline requirements for IoT security certification schemes

The fragmentation of the certification market has prevented the creation of consensus on a minimal set of fundamental principles of successful and usable schemes. It is necessary to identify the high priority market demands and develop the corresponding certification schemes to reduce the potential burden of a fragmented approach.

TIC Council members have extensive experience and understanding of existing cybersecurity testing and certification requirements, as can be illustrated by the voluntary certification schemes that members have developed and implemented, for example, based on ETSI EN 303 645 for consumer IoT products or Common Criteria testing.

TIC companies are well-positioned to assess the relevance of harmonised cybersecurity requirements. In this sense, TIC Council supports the list of essential requirements of the Cyber Resilience Act, Annex I which identify core principles for the security of connected devices that will pave the way towards building consensus in the market and support effort to reduce fragmentation.

4. Promoting the involvement of third-party conformity assessment bodies along the value chain to reinforce trust

Lack of knowledge and awareness on cybersecurity prevents a wider uptake of consumer IoT devices. The third-party TIC industry is essential to generate trust and transparency for end-users and public services.

Whether they are accidentally non-compliant products, false declarations of conformity or counterfeits, it is essential to have pre-market mechanisms in place. When performing conformity assessment activities, TIC companies are independent of commercial interests. In this way, the TIC sector ensures that no conflict of interest can lead to unscrupulous audit washing or issuance of certificates of conformity, which would prevent security and a level playing field.

Therefore, independent CABs allow early detection of non-compliant and potentially dangerous products on the market. Future IoT legislation should designate CABs (or NBs) in the conformity assessment activities they prescribe for certifying consumer IoT products. Upcoming cybersecurity legislations should emphasize the harmonised role of the TIC industry to support their effective implementation and assist manufacturers towards a cyber resilient world.

Annex I

Table of existing regulatory text mandating cybersecurity requirements for connected devices

Country	Name	Summary	Nature of the text	Involment of the TIC sector
China Ministry of Industry and Information Technology (MIIT)	IoT cybersecurity guidelines for the construction of basic security standard systems for the Internet of Things (2021)	Guidelines for the construction of basic security standard systems for the IoT with a focus on general security requirements and standardisation.	Voluntary guidelines Already into force.	No
EU	Cyber Resilience Act (Draft)	The Regulation is expected to set baseline harmonised requirements to all digital products following a risk-based approach.	Mandatory legislation + mandatory conformity assessment + fines The Regulation will fully enter into force in 2027.	Yes, with certification foreseen
EU	Cybersecurity Act (2019) + EUCC (2024) + other certification schemes under drafting	The Act reinforces the mandate given to ENISA and creates a new framework to develop voluntary cybersecurity certification schemes (CC, Cloud, 5G).	Voluntary certification schemes with 3 levels of assurance + data protection rules. Already into force.	Yes, but on a voluntary basis
EU	Delegated Act to the Radio Equipment Directive (2021)	The RED establishes a regulatory framework for the operation of radio equipment. The Delegated Act specifically addresses device requirements related to radio-specific issues ranging from common interfaces to cybersecurity.	Mandatory legislation to be followed by standardisation process. The delegated act will become mandatory on 1 August 2025.	Yes, but on a voluntary basis
India Telecommunication Engineering Center	Code of Practice for securing consumer Internet of Things (2021)	The report is expected to secure consumer IoT and set baseline requirements aligned with global standards and best practices.	Voluntary framework with baseline requirement without assurance levels. Already into force.	Yes, with certification foreseen
India Telecommunication Engineering Center	IoT Regulation on product labelling for TEC certification (2023)	The updated guidelines mandate new packaging requirements and update the list of products subject to mandatory certification.	National Centre for Communication Security body (NCCS) and TEC have made mandatory security testing and Certification of IP Router & Wi-Fi CPE. Both these products are mandatory from 01/01/2024.	Yes
Singapore Cyber Security Agency of Singapore (CSA)	Cybersecurity labelling scheme (2020)	First Asia-Pacific cybersecurity scheme under which consumer IoT are rated according to their levels of cybersecurity provisions.	Voluntary framework with 4 assurance levels: baseline requirements, label/certification and additional requirement for level 4. Already into force.	Yes, for level 3 and 4
United Kingdom Department for Digital, Media, Culture and Sport	The Product Security and Telecommunications Bill (2024)	A Bill about the security of internet-connectable products; about electronic communications infrastructure; and for connected purposes.	Mandatory framework with baseline requirement for internet-connectable devices. The Bill becomes mandatory on 29 April 2024.	No

Country	Name	Summary	Nature of the text	Involment of the TIC sector
USA Congress	H.R. 1668 - IoT Cybersecurity Improvement Act (2020)	Standards and guidelines for the federal government on the appropriate use and management by agencies of IoT devices, including minimum information security requirements for managing cybersecurity risks associated with such devices.	Mandatory framework mandating minimum security standards for IoT. Already into force.	No
USA - California California State Senate 2020	Senate Bill No. 327 - Information privacy: connected devices (2018)	Extend already existing privacy laws to connected devices and the information they collect, store, and transmit.	Mandatory framework, specify baseline requirement on uniqueness/ authentication of devices. Already into force.	No
USA – Oregon Oregon House of Representatives	House Bill 2395 (2019)	Requires manufacturer to equip connected device with reasonable security features that protect connected device and information that connected device stores from access, destruction, modification, use or disclosure that consumer does not authorise.	Mandatory framework with baseline requirements. Already into force.	No

Annex II

Conformity Assessment Approaches

	First-party conformity assessment	Third-party conformity assessment
WHAT	"Performed by the person or organisation that provides the object"[1] (i.e., supplier or manufacturer)	"Performed by a person or body whose interests in the product are independent from those of first parties and whose interests in fulfilment of requirements are independent from those of second parties"[2]
WHEN	A minimal level of risk associated with the non-compliance and with the product; Confidence that the manufacturer understands the technical, regulatory, and market requirements and has control over its supply chain; Fully funded post-market surveillance system that quickly and effectively removes non-compliant products from the market.	A higher risk associated with non-compliance and with the product; Need for an independent demonstration, for higher levels of confidence and assurance of compliance with the requirement; Manufacturer seeks to reduce in-house compliance costs or apply third-party as an added value to gain global market access and/or protect their brands and reputation; No fully funded market surveillance system.
HOW	The manufacturer itself states the conformity of its product with the applicable regulation and/or standard in a Supplier's Declaration of Conformity (SDoC). It requires significant investments in in-house testing capabilities and third-party testing can still be mandated in some cases.	The independent CAB performs conformity assessment tasks to verify that the product effectively [2] meets the requirements in the applicable normative text. If the object of conformity assessment respects all the mandatory clauses of such document, it is certified to be placed on the market; otherwise, it fails, and the manufacturer must redesign it: this is what is called a pass/fail system.

1. https://www.iso.org/standard/29316.html
2. https://www.iso.org/standard/29316.html

Annex III

IoT-related TIC Services

1. The TIC industry supports the overall legislative compliance of businesses and thus compliance with baseline cyber requirements

- Data privacy management and General Data Protection Regulation (GDPR) compliance audits, to ensure companies comply with regulations

2. The TIC industry participates in the continuous minimization of cyber risks and provides comprehensive approaches (assessment of safety, security, quality sustainability etc.)

- Cyber management assessment, to reduce risks attached to the supply chain
- Cyber risk management, including intrusion tests, to identify and mitigate company cyber risks

3. The TIC industry brings trust into the safe and secure operation of connected software and hardware and support access to markets

- Cyber management certification, to help companies assure their shareholders, investors and clients

TIC COUNCIL

Editor's Note About TIC Council

TIC Council is the global trade association representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together about 100-member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, medical devices, petroleum, mining and metals, food, and agriculture among others. Through provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and the wider TIC sector currently employs more than 1 million people across the globe.

TIC Council Secretariat
Rue du Commerce 20-22
B-1000 Brussels, Belgium
secretariat@tic-council.org
www.tic-council.org

Follow us online