Towards safe and secure connected devices

Striving for a safe and secure connected environment

Connected devices on the marketplace are expanding rapidly, both in number and in functionalities, which in turn provide immense possibilities. Nevertheless, they proliferate risk sources while users expect safety, privacy and security. The TIC Council (Testing, Inspection and Certification) welcomes policymakers' efforts to adapt the relevant regulatory framework to meet users' expectations. (see annex for examples of regulatory initiatives).

TIC Council recommendations for safe and trustworthy connected devices

1. Adopt a risk-based approach to conformity assessment

A risk-based approach to select the conformity assessment procedure for each type of device category would consider the device's intended use, foreseeable conditions of use, vulnerable users and apply specific security requirements, including related test methodologies for all assurance levels. In this context, involving third parties in the conformity assessment for connected devices should become mandatory according to a risk-based methodology.

2. Revise conformity assessment reflecting connected devices' evolving nature

Conformity assessment reports and certificates for connected devices should state their security and privacy scope, as well as their limitations, including minimal support duration and re-evaluation procedures to demonstrate continuous assessment, so that they are verified against newly discovered vulnerabilities and threats. In this context, the conformity assessment should include all relevant applications and backend systems.

3. Provide conformity assessment bodies with access to compliance-related data

Access to the devices' data that are related to safety, privacy and security is necessary for conducting conformity assessment, before the product is placed on the market, but also while it is in use. This is not limited to logging information. Security testing laboratories need to:

- conduct testing, inspections and controls while the device and related services are in use.
- receive enough information to acquire a clear understanding of the device's functioning and potential failures.
- remain informed about changes to connected devices, including software updates or upgrades, to assess their impact on product safety and information security.

Finally, to establish if a risk has materialised while in operation, manufacturers should equip devices with means to warn and log whether the device is compromised or is operating abnormally. This information about the operation of the devices should be recorded according to the risk analysis.

TIC Council
(formerly known as IFIA & CEOC)
Rue du Commerce 20-22 | B-1000 Brussels
secretariat@tic-council.org |+32 2 880 21 37
www.tic-council.org
BE 0724881295
Transparency Register No.: 840667012559

TIC Council Americas
2021 L Street NW, Suite 101-268, Washington, DC,
20036-4909, USA | +1 240 762 8069
Americas@tic-council.org | www.tic-council.org
TIC Council Americas, formerly known as IFIA Americas Committee

4. Ensure a holistic and global approach for connected devices' minimum requirements

In view of the pervasiveness of digitalisation to all products categories and the global interoperability expectations:

- It is important to establish a common industry framework protecting all users to increase awareness and promote the use of international standards.
- The requirements for placing products on the market should be revised to ensure that safety risks are addressed in conjunction with privacy and security in a technology-neutral manner. Overlapping requirements should be avoided.
- The regulatory framework should make use of internationally established risk classification systems and standards, offering a common global approach to security requirements for products. These can be used as guidance for defining cybersecurity requirements and related assurance levels.
- Boundary conditions of IoT systems should clearly define the requirements and responsibilities among all parties participating in an IoT architecture.
- Conformity assessment procedures should include at least validation of the secure development life cycle (SDLC) process, vulnerability assessment and penetration testing.
- Manufacturers should foresee the possibility to patch vulnerabilities discovered after the device's placement on the market with a conformity re-assessment procedure and establish an end-of-life programme. They should also provide relevant guidance.
- Compliance requirements should not refer only to the device and its development, but also the associated services and backend systems.

TIC sector contribution to connected devices

The TIC sector provides full testing, inspections, and certification services regarding, hardware and software implementation into connected devices and services, malicious code and penetration testing, cybersecurity connectivity, safety, electromagnetic compatibility and other requirements.

Manufacturers often engage TIC companies to provide a comprehensive review of their cybersecurity due diligence process throughout the devices' lifecycle. Thereby, the TIC sector contributes to manufacturers' "security by design" approach, which means that security is not only part of the final product, but an end-to-end approach throughout the complete supply chain including development, production, delivery, retail, personalization, use, until end of life.

TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification and verification organizations. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion.

TIC Council
(formerly known as IFIA & CEOC)
Rue du Commerce 20-22 | B-1000 Brussels
secretariat@tic-council.org |+32 2 880 21 37
www.tic-council.org
BE 0724881295
Transparency Register No.: 840667012559

TIC Council Americas
2021 L Street NW, Suite 101-268, Washington, DC,
20036-4909, USA | +1 240 762 8069
Americas@tic-council.org | www.tic-council.org
TIC Council Americas, formerly known as IFIA Americas Committee

Annex: Regulatory initiatives for connected devices in May 2020

- The EU is implementing the Cybersecurity Act, focusing on IoT devices, services and processes, while having already in place the General Data Protection Regulation (GDPR) securing personal identifiable information, eIDAS with a focus on electronic identification, authentication and trust services, the Payment Service Directive 2 (PSD2) for electronic transactions and the trust into payment service providers, as well as other relevant product-safety Directives. It also announced a strategy addressing safety, security, privacy and connectivity.
- In the United States, States have increasingly taken action to address issues of cybersecurity. On the federal level, proposals such as the Internet of Things (IoT) Cybersecurity Improvement Act of 2019 have been introduced, while reports, such as the Cyberspace Solarium Commission report recommend a National Cybersecurity Certification and Labelling Authority. Federal agencies have also taken action to provide guidance and to develop programs. The National Cybersecurity Center of Excellence (NCCoE) has published a number of guides and best practices and recently drafted the Security Review of Consumer Home IoT Products to inform readers about general considerations for improving the cybersecurity of consumer home IoT devices. The US Department of Defense (DoD), s working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification (CMMC) to ensure the security of the federal system.
- In India, the Information Technology Act (IT Act, 2000) deals with the implementation of security practices, the 'The Personal Data Protection Bill, 2019' seeks to provide protection of personal data of individuals and establishes a Data Protection Authority.
- The UK started with a Code of Practice for Consumer IoT Security in 2018 and is about to introduce a new Law to Strengthen Security of Consumer IoT Devices referencing ETSI global industry standard on good practice for cyber security in internet-connected devices EN303645. A related Test Standard TS103701 is in preparation.
- In Japan, the Basic Act on Cybersecurity Amended, has been implemented, while currently preparing a much broader Cyber-Physical Security Framework addressing the safety and cybersecurity of connected devices.