THE INTERNATIONAL TIC SECTOR WELCOMES THE PROPOSED MEASURES BY THE EUROPEAN COMMISSION AS A POSITIVE STEP TOWARDS SECURING THE CYBERSPACE

Cybersecurity is a topical issue, even more so in the wake of multiple recent security breaches. Digitalisation offers a wealth of opportunities; however, these can be hampered by security threats for citizens, industry, and governments alike. IFIA and CEOC International, on behalf of the independent third-party Testing Inspection Certification (TIC) sector, welcome the European Commission's proposal for a Regulation establishing a European Cybersecurity Certification Framework (the "Framework") for ICT products and services, including requirements for the essential functions and tasks of ENISA in the field of cybersecurity certification, that will help make the cyberspace safer for all stakeholders – including citizens and industry.

KEY SUCCESS FACTORS FOR A EUROPEAN CYBERSECURITY CERTIFACTION FRAMEWORK

- *Reliance on independent third-party conformity assessment and certification thereby increasing trust in and security of products and services.*
- *Mandatory certification for higher-risk products in the "substantial" and "high" assurance level categories to achieve the necessary levels of trust and security.*
- *Regulatory coherence of manifold cybersecurity regulations must be provided through cooperation to increase international acceptance and reduce duplicative requirements for manufacturers and service providers. Valuable committees like SOG-IS should be further enhanced.*
- *Effective regulatory framework, that allows for access to data for independent third-party Conformity Assessment Bodies and for requirements to verify "cybersecurity by design and throughout the product/service lifecycle" – there is no safety without cybersecurity*

INDEPENDENT CERTIFICATION PROVIDING TRUST IN CYBERSECURITY

Certification by independent third parties plays an important role in increasing trust in and security of products and services. As cybersecurity levels can neither be tested by the end user nor independently verified by the manufacturer, and public authorities often do not have the necessary internal resources, independent third-party certification can help meet this need in the most reliable and efficient manner. A cybersecurity certification scheme based on independent conformity assessment provided by accredited third parties will ensure an independent and impartial assessment of IoT products, processes and services. It will also provide demonstrable compliance that allows the users to have confidence in their choice of products and enables fair competition in the market.

ASSURANCE LEVELS BASED ON REQUIRED CONFIDENCE – CLEAR DISTINCTION BETWEEN MANDATORY AND VOLUNTARY CERTIFICATION

The certification framework must consider a clear distinction between critical, and therefore mandatory, certification processes and voluntary "duty of care" declarations. The interdependence of connected smart

IFIA – International Federation of Inspection Agencies
Rue du Commerce 20-22 | B-1000 Brussels
secretariat@ifia-federation.org | www.ifia-federation.org
EU Transparency Register: 840667012559-60

CEOC International Aisbl
Rue du Commerce 20-22 \ BE-1000 Brussels
info@ceoc.com \ www.ceoc.com
EU Transparency Register: 96818506624-46

products will significantly increase potential threats and vulnerabilities to society and the economy. A comprehensive certification framework must consider all of these new challenges.

Appropriate and accessible evaluation procedures must be established based on a thorough risk and threat analysis - both *what* is evaluated and *how* evaluation is performed shall be kept in mind when determining the appropriate conformity assessment procedures. When higher levels of assurance are necessary, the level of conformity must be more rigorous. The Framework must be designed in such a way that it ensures flexibility for cybersecurity certification schemes, to keep up with ever evolving risks and threats and introduction of new products, services and functionalities.

The introduction of basic, substantial, and high assurance levels, based on the specific cybersecurity needs, will provide users with the necessary information on cybersecurity properties. This will enable the objective determination of the level of security for a given ICT product, service or process.

Certain higher-risk products (e.g. connected and automated cars, electronic health, industrial automation control systems (IACS), Safety-Instrumented System (SIS), payment methods or smart grids), which would require a "high" level of assurance, should be subject to mandatory certification to achieve the levels of trust needed to support this Framework proposal.

Furthermore, it is necessary that products which require a "substantial" level of assurance should also be subject to a similar mandatory certification. These two types of categories and the product / service classification will depend on: the product's use case, the nature of the surrounding infrastructure, potential attackers' abilities over time, and even the consumer's awareness towards cybersecurity as a whole. Requirements for independent third-party certification in the "substantial" category will contribute to improved cyber resilience, not only at a product- or system- level, but also at an ecosystem level with IoT and IPv6 protocol connectivity expanding. Given the increasing interconnectivity between devices driven by the digital transformation it will be necessary to improve security in all devices, not only a few.

CREATING AN EFFECTIVE LEGISLATIVE FRAMEWORK – ACCESS TO DATA AS PREREQUESITE

The stipulated requirements for Conformity Assessment Bodies in Annex I are in line with common practices and with Regulation (EC) 765/2008. The same is true for the definitions used in Article 2 and throughout the Proposal, which are in line with existing Union legislation and internationally accepted standards. This ensures a clear and coherent regulatory framework to the benefit of all actors involved.

To assess the aspect of cybersecurity in an ICT product or service, the independent third-party Conformity Assessment Body will need full access to data, products and services, including their digital interfaces. The manufacturer, or service provider, assisted by independent third-party Conformity Assessment Bodies' agile verification processes should track and inform about changes to the IT components and services (e.g. software updates) so that continued compliance with the scheme requirements can be maintained.

NO SAFETY WITHOUT SECURITY

IFIA and CEOC International support the concept of "cybersecurity by design", but believe there need to be specific requirements that will verify both the process and the result. When independent third-party Conformity Assessment Bodies certify products for safety, additional cybersecurity aspects should be included, as there is no safety without (cyber) security. The earlier in the production chain that independent third-party conformity assessment is implemented, the more substantial will be the cost-efficiency for manufacturers and service providers. Potential design "defects" or irregularities can be identified and resolved at a very early stage before the product is in production and placed on the market, thereby improving the first time 'pass

rate' and avoiding costly recalls[1] and failures. Conflicts of interest are avoided as accreditation requirements prevent the independent third-party conformity assessment body that is assessing the conformity of a product, or service, from being directly involved in the design of those ICT products and services, thereby verifying that the certification body remains independent and impartial.

We advocate a review of the current (product) legislation using a risk-based approach to determine the potential risk of products and services and to assess and adapt the current conformity assessment procedure accordingly. This would close the regulatory gap that exists today, whereby the New Approach only addresses safety but not security aspects. When independent third-party Conformity Assessment Bodies certify products for safety they would need to also include cybersecurity aspects, as there is no safety without (cyber) security.

HARMONIZATION THROUGH CYBERSECURITY SCHEMES

A broad set of cybersecurity certification schemes currently exists, or are being proposed, across Europe and around the world with no unified or combined solution available. This makes a comparison between the services, products and systems difficult. Although there are already cybersecurity schemes in place today, they were designed for smaller scales, certifying only several hundred products per year. The proposed primacy of European cybersecurity certification schemes will lead to greater harmonization across the Single Market, thereby reducing the costs ("one-stop-shop") and time-to-market for manufactures by eliminating duplicative national requirements and providing greater transparency for all stakeholders involved.

It is of utmost importance to increase the development of high-level security standards. Therefore, valuable cybersecurity committees like SOG-IS need to be further enhanced since they provide the necessary standards and procedures for the demanded cybersecurity on product level.

INCLUSION OF PRE-EXISTING SCHEMES TO AVOID DISRUPTION IN THE MARKET AND MANAGE COSTS

The varying degrees of certification requirements coupled with many different approaches to standardisation frameworks have resulted in a fragmentation of the Single Market. These obstacles incur duplicative costs for manufacturers, operators and uncertainty for consumers. Harmonized cybersecurity certification referring to common standards or criteria of evaluation and testing methodologies will allow higher efficiency levels and lower costs for market participants. Furthermore, these mechanisms are more efficient when conducted by independent Conformity Assessment Bodies, which support industry in meeting the needs of building trust and verifying the security of their products and services.

We support a single European cybersecurity certification scheme over multiple national schemes with the same scope. To avoid disruption of the market we encourage a solution that would allow pre-existing schemes with the same scope and assurance level, to be merged into the respective new European cybersecurity certification schemes to allow for a smooth transition for the users.

IMPROVING INTERNATIONAL ACCEPTANCE THROUGH COOPERATION

In today's connected, globalised world international cooperation on cybersecurity is essential to trade and to ensure high levels of security to users. Therefore, we support that the schemes proposed in the future Framework should allow for cooperation with third countries and rely on international standards to avoid creating trade barriers. Fostering regulatory coherence and improved regulatory cooperation, including

[1] Internal studies carried out by IFIA members have shown that for products that were submitted to an independent third-party, the rejection rate of first-time submittals for not meeting safety requirements was on average 50%. These were products that were submitted after the manufacturers had carried out their own internal conformity assessment and the product (providing no Notified Body involvement was required) could therefore have been placed on the market. http://ceoc.com/documents/CEOC%20Gitte%20Schjotz.pdf

working towards greater harmonisation in standards, and broader recognition and use of international standards, may result in reducing the required testing and certification costs, thereby providing a benefit to manufacturers across the globe.

Reliance on internationally accepted standards, including accreditation standards and requirements, will lead to greater regulatory coherence and will allow European manufacturers, service providers and Conformity Assessment Bodies to be active in a global market place. The adoption of internationally recognized schemes as European schemes should be considered (similar to the adoption of ISO standards as EN standards).

ENSURING A LEVEL PLAYING FIELD FOR CONFORMITY ASSESSMENT BODIES

To achieve a consistently high level of cybersecurity across the Single Market, it will be necessary to ensure a level playing field for Conformity Assessment Bodies. Due to the characteristics of cybersecurity certification and the dynamic developments in that area, widely established mechanisms such as peer assessments should be considered in addition to accreditation. A good example is the IECEE Peer Assessment Programme [1] that has a proven track record of creating the necessary high levels of confidence among the participants.

CLEAR RESPOSIBILTIES FOR ALL ACTORS INVOLVED

To ensure the functionality of the system and to avoid conflicts of interests, manufacturers, services providers, Conformity Assessment Bodies as well as national certification supervisory authorities need clearly defined roles and responsibilities in line with the New Legislative Framework. Such a clear division of duties enhances the necessary confidence in the entire system, ensures regulatory coherence and enables fair, clear and transparent competition conditions in Europe.

PERMANENT STAKEHOLDERS' GROUP

With their global footprint and technical expertise, our members already provide independent third-party security evaluation, testing, inspection, and certification services against clear regulatory frameworks and harmonized standards across a variety of areas and industries. We are ready and willing to share our experience with the Permanent Stakeholders' Group, to support the development of an effective harmonized approach to security testing and certification. The Permanent Stakeholders' Group should be established in a similar manner as the IEC Conformity Assessment Board, where representatives from industry, Conformity Assessment Bodies, and government are part of the scheme management and work in unison to insure effective results.

THE ROLE OF INDEPENDENT THIRD-PARTY CONFORMITY ASSESSMENT BODIES AND THE TIC SECTOR

Given the high risk linked to cybersecurity, any certification mechanism needs to be designed to meet three key objectives:

- Protecting the end user from any damage regarding the device's confidentiality or integrity.
- Protecting data security and confidentiality, and against data corruption.
- Avoiding low risk and mass market goods to be turned into weapons against critical infrastructures.

It is important to note that independent third-party TIC companies can help effectively meet these objectives. They have the required technical competence, and have no conflict of interest due to a lack of financial gain

associated with the outcome of the evaluation for compliance. Independence and competence of third parties are based on the ISO/ IEC 17000 series of standards, which provide the requirements to which independent third parties must adhere. These accreditation requirements are recognised worldwide and thus facilitate cross border acceptability of products and services.

Regarding performance and competence, TIC companies provide services to a wide range of industry sectors across the world with a variety of differing requirements. With more than 100 years of experience, the independent third-party TIC organizations have developed knowledge, competence and expertise in various sectors. Thanks to the broad range of services they provide, these TIC organizations are positioned to support technological progress and innovation in a myriad of sectors while supporting compliance with national and international standards and regulations. The independent third-party TIC sector has partnered with industries and government in the past to support the first industrial revolution; today it has the ability and experience to help implement the proposed EU Cybersecurity Certification Framework and to contribute to the transition towards this next digital revolution.

On behalf of our members from the independent TIC sector, IFIA and CEOC International would be pleased to discuss our views as outlined above and to offer expertise to support the implementation of this ambitious project that will support the protection of European economies against the threats of cyber-attacks while fostering trust in IoT products and services

ABOUT IFIA AND CEOC INTERNATIONAL

Founded in 1982, the International Federation of Inspection Agencies (IFIA) is the federation of organisations that provide inspection, testing and certification services internationally. IFIA currently represents around 60 of the world's leading international testing, inspection and certification bodies representing over 300,000 employees and a combined turnover of roughly €23 billion.

Created in 1961, the International Confederation of Inspection and Certification Organisations (CEOC International), is the European trade association representing 29 members from 19 countries. Members are active in over one hundred countries around the world creating a truly international dimension. CEOC International members are accredited by public authorities to provide inspection, auditing and conformity assessment services for a wide variety of products and systems.