CEN – European Committee for Standardization
CENELEC – European Committee for Electrotechnical Standardization

CEN Identification number in the EC register: 63623305522-13
CENELEC Identification number in the EC register: 58258552517-56

CEN and CENELEC Position Paper on the draft regulation ''Cybersecurity Act''

January 2018

Background

The European Commission released on the 13th September 2017 the “Proposal for a Regulation of the EP and the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification” (‘Cybersecurity Act’) [COM (2017) 477].

With this document, CEN and CENELEC provide their input to the ongoing discussions in the European Parliament, Council of the European Union and the European Economic and Social Committee on the above-cited communication.

Executive summary

CEN and CENELEC welcome the proposal made by the European Commission for a Cybersecurity Act [COM (2017) 477] as part of its cybersecurity strategy to avoid purely national solutions and look forward to working together to address the current fragmentation of the European market. To ensure a coherent European approach to cybersecurity CEN and CENELEC stress the importance to:

- **Define** what is meant by ‘ICT products and services’ covered by the proposal, and formally engage with the European Standardization Organizations (ESOs) to establish a priority list of products, services and digital competences and qualifications so that standardization can timely accompany market needs.
- **Invite** the formally recognized national, European and international standardization organizations (as per Regulation 1025/2012) to define the requirements and standards to be used in the certification schemes. Where applicable, priority should be given to International Standards, which enable European industry to access global markets.

Rue de la Science 23 - 1040 Brussels - Belgium
Tel: +32 2 550 08 11 - Fax: +32 2 550 08 19 – info@cencenelec.eu - www.cencenelec.eu

- **Apply** the process of the New Legislative Framework (NLF), which provides a clear separation between legislation, standards, and conformity assessment and avoids creating a new practice, which would cause confusion in the market place.
- **Revise** the technical details included within the security objectives and the assurance level sections, in order to make them fully applicable to real use cases and coherent with modern best practices.

CEN and CENELEC contribution

To ensure a coherent European approach to cybersecurity CEN and CENELEC stress the importance to:

1) **DEFINE what is meant by 'ICT products and services' covered by the proposal and formally engage with the European Standardization Organizations (ESOs) to establish a priority list of products, services and digital competences and qualifications so that standardization can timely accompany market needs.**

European Standards are valuable tools – voluntary and strongly founded on the WTO/TBT principles – for the promotion of best practice, increased efficiency, interoperability, and better quality of products and services in all business sectors. They are proven assets to the development of the Single Market and are used as a tool in support of European legislation and public policy: CEN, CENELEC and ETSI are recognized by Regulation 1025/2012 as European Standardization Organizations (ESOs), providing voluntary European Standards (ENs).

With the new proposal, the European Commission states its intention to reinforce and preserve the security of ICT products and services and to increase trust in their use by the EU citizens.

CEN and CENELEC share the view that the current proposal provides insufficient information on the ICT products and services intended to be covered by the upcoming EU certification framework, while not addressing the digital competences and qualifications required to respectively operate and use them.

A majority of products and services currently placed on the market are ICT–enabled. The scope of the new regulation needs to clearly set the boundaries of the ICT products and services that will be covered by the new certification schemes, and the main digital competences and qualifications that interact with them throughout the products and services lifecycles. Different security levels should be defined according to the need of users for trust and confidence (be it B2C, B2B or Critical Infrastructures). Conformity assessment methods need to be adapted to the different risk levels.

CEN and CENELEC therefore invite the European Commission to set out a coherent, risk-based approach in defining a list of products, services and/or digital competences and qualifications to which the certification schemes would apply first, whilst keeping in mind that the usage of certification schemes should be allowed regardless of the technology.

European Standards could support the envisaged certification schemes, reflecting interactions and interdependence along the whole value chain in the ICT industry and for the benefit of all business sectors, while taking into account the broadest spectrum of stakeholders. Any framework should take into account existing standards that are already widely accepted, such as the Common Criteria (ISO 15408), the requirements and information security management for IT (ISO/IEC EN 27000, 27001, 27002), industrial automation and control systems (IEC 62443), and industry sector-specific standards.

The European Standardization System enables the engagement all stakeholders: policy makers, societal, consumers and SMEs (Annex III organizations as defined by Regulation 1025/2012), and industry to collect requirement needs that could become part of European or International Standards on data protection, information protection and security techniques with specific focus on cybersecurity covering all aspects of the evolving information society. The use of International and European Standards guarantees openness, ensures broad stakeholder participation to the benefit of consumers and SMEs (as proven in CEN-CENELEC Joint Technical Committee (JTC) 13 'Cybersecurity and Data Protection'), and leaves room for future innovations.

2) **<u>INVITE</u> the formally recognized national, European and international standardization organizations (as per Regulation 1025/2012) to define the requirements and standards to be used in the certification schemes. Where applicable, priority should be given to International Standards, which enable European industry to access global markets.**

The primary objective of standardization is the definition of voluntary technical specifications with which current or future products, production processes, services or digital competences and qualifications may comply. Standardization can cover various issues, such as different grades or sizes of a particular product or technical specification where safety, efficiency, compatibility, and interoperability with other products or systems are essential.

European Standards are established through a transparent, balanced, and consensus-based process where all stakeholders are invited to contribute (including ENISA's representatives and experts, consumers and SMEs). Therefore, CEN and CENELEC should be involved in developing standards as basis for testing and evaluation in certification schemes following the established standardization process as defined by Regulation 1025/2012. This will foster stakeholders' commitment, the link between European and International Standards as well as coherent national implementations of European cybersecurity requirements to ensure the technical consistency of the Single Market.

The long-standing cooperation of the ESOs with ISO, IEC and ITU-T has allowed the alignment of European Standards with international ones, contributing to the global competitiveness of European businesses. Strengthening this cooperation in cybersecurity as well, will facilitate the development of ISO and IEC standards to support European legislative and policy needs. It will also secure EU businesses involvement in the definition and implementation of EU certification framework.

Specific requirements developed by the European Commission or ENISA - in parallel to European and/or International Standards - would create competition with these standards, create uncertainty and ultimately stifle innovation.

Therefore, CEN and CENELEC recommend, wherever possible, to make use of International Standards for testing and evaluation in the certification schemes to ensure certification against well-proven, community-approved technical specifications.

3) APPLY the process of the New Legislative Framework, which provides a clear separation between legislation, standards, and conformity assessment and avoids creating a new practice, which would cause confusion in the market place.

For more than 30 years, the ESOs have developed harmonized standards, which manufacturers, economic operators, or conformity assessment bodies can use to demonstrate that products, services, or processes comply with relevant EU legislation. CEN and CENELEC have developed standards in all business sectors and for use in a variety of purposes. By definition, European Standards are voluntary and organizations that use them do so voluntarily.

We believe that the conformity assessment system, provided by the New Legislative Framework, should be the preferred solution for the implementation of the new cybersecurity solutions. For products subject to harmonized regulation (e.g. medical devices, aviation, toys, electrical equipment, construction or measuring instruments), any scheme introduced by the future EU cybersecurity framework should fit seamlessly with existing ways to assess and demonstrate compliance with the legal framework, and allow for self-assessment. This approach has proven to be an efficient and effective tool to make high-risk products safe across Europe, which consumers can trust.

CEN and CENELEC urge the European Commission to apply Regulation 1025/2012[1] when defining the requirements for ICT products, services and digital competencies and qualifications and reuse as much as possible the existing certification schemes instead of establishing a parallel

[1] Also in the context of: Regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products, and Decision No 768/2008/EC of the European Parliament and of the Council on a common framework for the marketing of products

system for certification. The current proposal might lead to the establishment of a new practice and parallel system to the recognized standardization system, which will hamper the take-up of new solutions and technologies rather than increase trust or security of product and services.

The upcoming regulation should clarify how the scheme's cybersecurity requirements will be established. Cybersecurity is an international challenge. International Standards – and European Standards based on International Standards - provide the basis by which the European export-driven industry can access global markets. The international standards system avoids national and regional technical particularities that lead to technical barriers to trade. To achieve a consistent and effective EU certification framework for cybersecurity, European and International Standards will need to play a crucial role.

4) **REVISE the technical details included within the security objectives and the assurance level sections in order to make them fully applicable to real use cases and coherent with modern best practices.**

Technical cybersecurity details to be included in the regulation should be minimal and precise in order not to incur the risk of being not exhaustive or imprecise. Therefore, detailed considerations about security objectives should be generalized and left up to the certification schemes. The same consideration holds true for the assurance levels to be included and the criteria governing them.

General requirements should be given, like mandating a risk-based approach or using management systems structures and vocabulary when feasible. If any technical indication is needed then the involvement of the ESOs will be crucial as they have the experience of working on this type of technical requirements.

About CEN and CENELEC

The **European Committee for Standardization ("CEN") and the European Committee for Electrotechnical Standardization ("CENELEC")** are two officially recognized European Standardization Organizations under Regulation 1025/2012 on European Standardisation[2].

CEN and CENELEC develop European Standards (ENs) and other technical deliverables through a transparent and consensus-driven process to meet the needs of European stakeholders, such as industry and service providers, including SMEs, public authorities and regulators, academia, research centres and societal stakeholders' organizations.

In addition, CEN and CENELEC provide a platform for the development of *harmonized* European Standards (hENs) that may incorporate quality, safety, environmental, interoperability and accessibility requirements to support the implementation of the relevant European legislation.

CEN and CENELEC membership is composed of national standardisation bodies from 34 countries, whose national networks involves more than 100 000 technical experts from industry, business and commercial federations (including SMEs), research, consumer organizations, environmental groups and other societal stakeholders. For more information, please see: www.cencenelec.eu

CEN and CENELEC Cybersecurity activities:

CEN-CENELEC/JTC 13 'Cybersecurity and Data protection'
CEN-CENELEC/JTC 8 'Privacy management in products and services'
CEN/TC 278 'Intelligent transport systems'
CEN/TC 301 'Road vehicles'
CEN/TC 377 'Air Traffic management'
CEN/TC 428 'Digital competences and IT professionalism'
CENELEC/TC 8X 'System aspects of electrical energy supply'
CENELEC/TC 9X 'Electrical equipment and systems for railways' (Smart Cars)
CENELEC/TC 13 'Electrical energy measurement and control'
CENELEC/TC 205 'Home and Building Electronic Systems'
CENELEC/TC 59X 'Consumer information related to household electrical appliances'
CEN/BT WG 220 'Fintech'
CEN-CENELEC Focus Group on 'Blockchain and distributed ledger technologies'
CEN-CLC-ETSI Coordination Group 'Smart Energy Grids'
CEN-CLC-ETSI Coordination Group 'Smart Meters'

[2] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 316, 14.11.2012, p. 12–33