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

Discussion Paper

Cybersecurity Act 2

Regulation on ENISA, the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881

Executive Summary

In the Cybersecurity Act 2, CEN and CENELEC urge the Commission to:

- **ensure that standards developed by the ESOs are maintained as the backbone of cybersecurity certification schemes.**
- **confirm that technical specifications developed by ENISA remain a last resort fallback option. The Article on Common Specifications from the Toy Safety Regulation could be used as inspiration for framing the use and development of ENISA technical specifications.**
- **start a dialogue with the ESOs regarding the exclusion of high-risk suppliers from the European technical committees developing cybersecurity standards.**

1. Introduction

CEN and CENELEC welcome the Cybersecurity Act 2 (CSA 2) with the aim of strengthening cybersecurity governance in the Union and supporting the development of a secure, resilient and competitive digital single market. ENISA has played a crucial role in developing standards for the Cyber Resilience Act within the ESOS by providing technical input as well as assessments of the draft standards to ensure their alignment with the essential requirements. A more active and coordinated contribution from ENISA can further support the development of timely, relevant and high-quality European standards that are coherent across legislations.

2. Strengthening the mandate of ENISA in the field of standardization

The proposal establishes a renewed European framework for cybersecurity certification schemes (ECCF). These certification schemes provide companies and organizations with voluntary tools to demonstrate compliance with cybersecurity requirements under

existing regulation. It is essential that these schemes continue to be based on European standards, also based on international ones, developed by the European Standardization Organisations (ESOs) through a bottom-up approach driven by technical experts across Europe, as this ensures up-to-date, technologically neutral and market relevant basis for certification schemes.

The proposal however expands ENISA's mandate in the field of standardization by allowing ENISA to draft their own technical specifications for certification schemes. This marks a concerning shift away from the clear allocation of responsibilities set by the public-private partnership, where regulatory requirements are set by the European institutions and technical standards developed by the ESOs.

The motives for such an expansion are not adequately explained in the proposal. ENISA is already actively contributing to standardization activities within CEN and CENELEC, which raises the question of why developing parallel technical specifications outside the established ESO system would be necessary.

This expansion also contradicts ongoing efforts to modernize and strengthen the European Standardization System (ESS). CEN and CENELEC are actively working to become more agile by offering a path to integrate diverse and wide-ranging technical inputs from outside the ESS in a structured way, as well as developing new deliverables with a faster time to market.

The ESOs provide a well-established, internationally recognized system built on WTO principles, involving 90,000 technical experts from a wide range of stakeholders. European standards are uniformly adopted across all 34 CEN and CENELEC Members and support international alignment through the close cooperation with ISO and IEC.

ENISA drafting its own technical specifications would require considerable new resources and create unnecessary duplication. It would bypass the established systems and processes already in place within the ESOs, risk fragmentation of the European standardization landscape, and dilute the limited resources of experts who participate in developing European standards that could lead to reduced stakeholder involvement.

To ensure coherence and consistency these specifications should be framed with clear criteria, as is the case with Commission developed common specifications.

- **The Cybersecurity Act 2 should ensure that standards developed by the ESOs are maintained as the backbone of cybersecurity certification schemes.**

3. Framing ENISA technical specifications

The proposed Omnibus IV harmonizes the consistent application of common specifications across legislations. Therefore, applying the same criteria to ENISA's

technical specifications would ensure consistency between the CSA and other legislations.

Technical specifications drafted by ENISA should:

- Remain very exceptional
- Be a fallback solution, as in the case of common specifications
- Involve all relevant stakeholders
- Establish when these should be withdrawn (especially as soon as a harmonized standard is available or if a Member State objects)

CEN and CENELEC recommend the Commission to take inspiration from Article 14 on common specifications of the Toy Safety Regulation (2025/2509) (Annex I) to outline ENISA technical specifications. This Article forms the basis of the Council's negotiating mandate on the Omnibus IV and is preferred by a wide range of stakeholders because it clearly defines the above points, in particular the fact that:

1. Common specifications can only be issued when

- there is no harmonised standard covering the requirements published in the OJEU and no such reference is expected to be published within a reasonable period.
- a standardization request has been issued by the Commission, but the European Standardization Organizations rejected it.
- the standards requested have not been delivered within the set deadline.
- the standards requested do not comply with the request.
- the standards requested do not satisfy the requirements they aim to cover.

2. The Article also foresees

- consultation with all relevant stakeholders.
- common specification or parts thereof to be repealed or amended when reference of a harmonised standards that cover the same essential safety requirements is published in the OJEU.
- possibility to amend the common specification when Member State considers that the essential safety requirements are not entirely satisfied.

Unfortunately, Article 77 that outlines ENISA technical specifications do not include any of these essential safeguards. This creates misalignment across legislations and grants the European Commission and ENISA wider margin to interpret when to use these technical specifications developed outside the ESOs.

- **The Cybersecurity Act 2 should confirm that technical specifications developed by ENISA remain a last resort fallback option. The Article on Common Specifications from the Toy Safety Regulation could be used as inspiration for framing the use and development of ENISA technical specifications.**

4. Limiting high-risk suppliers access to standardization processes

Article 100 (4) in the proposal restricts high-risk suppliers access to *"participate in the development of, assessment, consultation or decisions concerning European standards and European standardization deliverables…"*.

While we understand that there might be specific cases where for security reasons the Commission might need to exclude certain high-risk suppliers access, CEN and CENELEC are concerned about the precedent that Article 100 (4) sets to restrict participation in standardization processes in overarching legislations.

The ESS is built on the WTO principles of transparency, openness, impartiality, consensus, effectiveness, relevance, and coherence that serve as the global mandate for open, fair, and trusted standardization. Furthermore, the national delegation principle that is the basis of CEN and CENELEC ensures that the position taken by national standard bodies reflect a balanced national position rather than individual positions.

Removing high-risk suppliers according to the current Article 100(4) would be a huge administrative burden to national and European standardisation bodies, and without guaranteeing the actual exclusion of high-risk suppliers interests.

Restricting participation in the 'consultation' of draft European standard would be detrimental to the enquiry stage of the standard development process. The enquiry stage allows the entire public, including ones who have not been participating in the development of the standard, to provide their comments on the draft ensuring an inclusive process and standards that are open and transparent.

In addition, identifying the majority interest and ownership behind each individual input provided through the public enquiry would be impossible for the national standardisation bodies. In any case the national mirror committees consolidate the comments and provide a cohesive input to the European technical committee.

Any restriction on stakeholder participation should be implemented in close dialogue and cooperation with the ESOs. This is necessary to ensure transparency, legitimacy, and continued trust in European standardisation processes.

To better reflect the considerations laid out above, CEN and CENELEC propose the following wording for Article 100(4):

"High-risk suppliers shall not be entitled to:

(a) participate in the development of ~~assessment, consultation or decisions~~ ~~concerning~~ European standards and European standardisation deliverables, ~~referred~~ <u>if requested under</u> ~~to in~~ Article 10(1) of Regulation (EU) 1025/2012, and common specifications referred to in Article 27 of Regulation (EU) 2024/2847 in the area of cybersecurity;"

- **The Commission should start a dialogue with the ESOs regarding the exclusion of high-risk suppliers from the European technical committees developing cybersecurity standards.**

Annex 1: Toy Safety Regulation (2025/2509) Article 16

Article 16 ***Common Specifications***

1. Toys which are in conformity with the common specifications referred to in paragraph 2 or parts thereof shall be presumed to be in conformity with the essential safety requirements to the extent that those requirements are covered by those common specifications or parts thereof.

2. In exceptional cases, the Commission may adopt implementing acts establishing common specifications covering requirements that provide a means to comply with the applicable essential safety requirements.

Those implementing acts shall only be adopted where the following conditions are fulfilled:

(a) there is no harmonised standard covering the applicable essential safety requirements the reference of which is published in the Official Journal of the European Union and no such reference is expected to be published within a reasonable period; and
(b) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft or to revise European standards for the applicable essential safety requirements and:
    (i) the request has not been accepted by any of the European standardisation organisations to which the request was addressed; or
    (ii) the request has been accepted by at least one of the European standardisation organisations to which the request was addressed, but the European standards requested:
    -are not delivered within the deadline set in the request;
    -do not comply with the request; or
    -do not satisfy the requirements they aim to cover.

The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 53(3).

3. Before preparing a draft implementing act as referred to in paragraph 2 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers that the conditions in that paragraph have been fulfilled.

When preparing a draft implementing act as referred to in paragraph 2 of this Article, the Commission shall take into account the views of the Expert Group on Toys Safety and shall consult all relevant stakeholders.

4. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal or amend the implementing acts referred to in paragraph 2 of this Article, or parts thereof, which cover the same essential safety requirements as those covered by that harmonised standard.

5. Where a Member State considers that a common specification does not entirely satisfy the essential safety requirements, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, where appropriate, amend the implementing act establishing the common specification in question.

About CEN and CENELEC

CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) are recognized by the European Union (EU) and the European Free Trade Association (EFTA) as European Standardization Organizations responsible for developing standards at European level, as per European Regulation 1025/2012. The members are the National Standards Bodies (CEN) and National Electrotechnical Committees (CENELEC) from 34 European countries. European Standards (ENs) and other standardization deliverables are adopted by CEN and CENELEC, are accepted and recognized in all of these countries. These standards contribute to enhancing safety, improving quality, facilitating cross-border trade and strengthening of the European Single Market. They are developed through a process of collaboration among experts nominated by business and industry, research institutions, consumer and environmental organizations, trade unions and other societal stakeholders. CEN and CENELEC work to promote the international alignment of standards in the framework of technical cooperation agreements with ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission).