European Committee of Electrical Installation Equipment Manufacturers

11th May 2018

POSITION PAPER

CECAPI opinion about the Draft European Regulation Cybersecurity Act

1. EXECUTIVE SUMMARY

In September 2017, the European Commission published a proposal for a Regulation of the European Parliament and the Council on Information and Communication Technology (ICT) cybersecurity certification referred to as the "Cybersecurity Act".

CECAPI welcomes this proposition to harmonize ICT certification approaches at European level. It specifically welcomes the voluntary nature of such certification.

This position paper highlights some points that CECAPI believes should be further elaborated and clarified in the proposed Regulation, summarised below.

- ✓ Clarify the **Governance** to ensure relevant stakeholders from the industry have been engaged
- ✓ Revise the defined **assurance levels** to best align to existing levels, and to **integrate self-declaration** complimentary to certification.
- ✓ Enable the development and use of international and European **standards**
- ✓ Clarify and harmonize the system of **penalties** across the union

About CECAPI

CECAPI is the European Committee of Electrical Installation Equipment Manufacturers. Its objective is to promote & develop common technical, industrial, economic and political interests of the European electrical installation equipment industry.

All equipment and components for electrical installations for residential and commercial use fall within its scope (including but not limited to: Components for electrical installations and appliances, Cable management systems, Home & building electronic systems, Intercom & video-intercom, Circuit breakers, Residual current devices)

POSITION PAPER

2. GOVERNANCE TO ENSURE RELEVANT STAKEHOLDERS FROM THE INDUSTRY HAVE BEEN ENGAGED

ARTICLES 8, 46

Within the tasks requested from Enisa in the proposed Regulation, it is identified that it shall cooperate with the industry (Article 8). However, the inclusion of the industry in the definition of certification schemes, and the process on which it should rely on to engage with the industry stakeholders is unclear.

In addition, the certification levels definitions (Article 46) are too vague to be understood by end customers as is, or provide any clear differentiating factor that can easily be understood by users. A certification to a certain level can never completely eradicate the risk or a cybersecurity incident to that product or service, as this will also depend on multiple factors as the configuration or implementation or the product or service within a specific scope. These certifications could have consequential benefits to increase trust, but can very quickly be hindered and prove useless if they are not accompanied with the correct level of awareness to users.

CECAPI recommends that the proposed Regulation further clarifies the processes and governance by which ENISA will ensure:

- The industry can give input to proposed certification schemes to avoid unpractical or inapplicable schemes
- Certification levels and their coverage are understood by users to avoid the false sense of security

POSITION PAPER

3. REVISE THE DEFINED ASSURANCE LEVELS — ARTICLE 46

Three levels of assurance are defined (Article 46): basic, substantial and high.
It is to be noted that depending on the functions ICT of products and services, and the context of use of such products and services, the equivalence of assurance levels would be difficult to define.
The requirements for an ICT product or service should be based on a risk approach, specific to each ICT product or service within its scope of use, and depending on the vertical it falls into.
To illustrate, taking for example some extremes, an Industrial Control System and a connected home appliance could both be certified at an assurance level “substantial”, but would require significantly more or less effort, means, and measures to reach such a level.

In addition to the fact that the differences between those levels are unclear, and should be clarified, existing standards and processes (for example IEC 62443 series, ISO/IEC 15408) already include security levels and assurance levels, and are difficult to match to the levels defined within this regulation.

Taking example on existing mechanisms already in place and effective in the union, and largely used within the industry, it also seems necessary to redefine the levels to include self-declaration of conformity as complementary approach to certification.

CECAPI recommends and would welcome that the proposed Regulation:

- Requires different levels of security and different ways to assess those levels depending on the products
- Aligns or matches the levels with existing and commonly used levels in the industry
- Integrates self-declaration of conformity as a complementary approach to certification, reflecting the level of security measures implemented instead of the supposed assurance level.

POSITION PAPER

4. USE OF STANDARDS — ARTICLES 8, 46

One of the tasks requested to Enisa is to "facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products and services" (article 8).
Standards are referenced in the assurance levels defined (article 46) and must serve as a basis to define the certification schemes. Companies that would benefit from union wide certification schemes would potentially also require those to go cross union borders, and it is necessary to privilege International standards when those exist or the development of such standards leveraging existing agreements between European standardisation bodies and international standardisation bodies (Vienna agreement and Frankfurt agreement).

In view of the apparent lack of standards in some verticals, it is also urgent to define a priority list of requirements to standardisation bodies, and ensure coherence between what those standards define and the requirements of this Regulation.

CECAPI recommends that the proposed Regulation:

- Require Enisa to define a list of priority verticals to be addressed by European and International standardization bodies
- Clarify the role of standardization bodies in the development of standards relating to the regulation

5. CLARIFY AND HARMONIZE THE SYSTEM OF PENALTIES — ARTICLE 54

The regulation, throughout a certification process, implicates directly or indirectly several bodies, including Enisa, National certification supervisory authorities, national accreditation bodies, conformity assessment bodies, ICT product manufacturers and ICT service providers.

The rules on penalties to infringement of certification schemes are to be set under the responsibility of member states (Article 54), it is however unclear to whom those penalties apply, and specifically, if a certification has been granted and is proven unreliable, who would be responsible.

The understanding of this specific aspect could vary from a national body to another, and would greatly hinder the validity and interest in a cross-union certification.

CECAPI recommends that the proposed Regulation
- Clarifies which cases are considered for penalties and who those penalties apply to.