ETSI Position Paper on draft Regulation 2017/0225 ''Cybersecurity Act”

Preamble

In September 2017, the European Commission published a 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 (ICT) cybersecurity certification ("Cybersecurity Act")".

ETSI welcomes the overall objective of the proposed Regulation to “increase EU resilience, enhance its cybersecurity preparedness and avoid fragmentation of certification schemes in the EU”.

This position paper highlights some points that ETSI believes should be further elaborated and clarified in the proposed Regulation, namely:

1. **Standards for certification: clarify concepts and definitions**
2. **Use the New Legislative Framework as a toolbox**
3. **Rethink the three levels of security with a risk management approach and rethink the way objectives are described**
4. **Ensure applicability and consistency with existing regimes**
5. **Specify governance and processes**

About ETSI

ETSI provides members with an open, inclusive and collaborative environment to support the timely development, ratification and testing of globally applicable standards for ICT-enabled systems, applications and services across all sectors of industry and society.

We are a not-for-profit organization with more than 800 member organizations worldwide, drawn from 65 countries and five continents. Members comprise a diversified pool of large and small private companies, research entities, academia, government and public organizations.

ETSI is one of only three bodies officially recognized by the EU as a European Standards Organization (ESO).

1. Standards for certification: clarify concepts and definitions

There is no effective certification without standards.

Standards define and clarify methods and processes by which secure systems can be built and how essential requirements can be fulfilled. Standards developed using open and consensus –based processes, provide a solid foundation for all stakeholders. Industry can implement these standards into products and technology offerings and do accurate and robust development accordingly.

Certification without having clear standards against which certification is performed creates obscurity and uncertainty for market players, public authorities and ultimately end users.

Regulation (EU) No 1025/2012 is the primary EU standardisation legislation and gives definitions for reaching compliance with requirements of standards, technical specifications and ICT technical specifications.

A certification scheme, as proposed in the draft Regulation needs to identify a standard, technical specification or ICT technical specification which forms the basis for reaching a certain level of cybersecurity and meet respective cybersecurity requirements.

This process should explicitly follow the procedure as defined in ISO/IEC 17067:2013[1] chapter 6 which describes the "Development and operation of a product certification scheme". According to this international standard, a certification scheme should specify "the requirements against which the products are evaluated, by reference to standards or other normative documents (…)".

ETSI recommends that this fundamental relationship between standards and certification schemes is unambiguously and explicitly described in the draft Regulation.

[1] Conformity assessment — Fundamentals of product certification and guidelines for product[1] certification schemes

2. Use the New Legislative Framework (NLF[2]) as a toolbox

In the Single Market, the New Legislative Framework (formerly referred to as "New Approach") laid down the rules and processes for gaining market access in Europe and for operating under the Presumption of Conformity:

(i) Essential/core requirements are set by governments/regulators;

(ii) Standards are developed alongside WTO-TBT principles[3] by all interested parties, whether public or private entities, defining methods and processes for how to meet the requirements;

(iii) Conformity Assessment (including self-assessment) may be carried out against the relevant standard, confirmed in a supplier's Declaration of Conformity on which basis market access to the European harmonised market is granted on the basis of the Presumption of Conformity.

The process of the NLF provides a clear approach regarding requirement setting – standardisation – conformity assessment.

This includes self-assessment which is, therefore, a proper process in Europe and is applied very rigorously. Self-assessment has worked well for many decades in regulated areas such as product safety and other technical fields.

It is also very much the model followed in the digital and ICT environments which are germane to cybersecurity- while some cybersecurity domains adopted 3rd party assessment. In order to have synergy and consistency with the European and global digital markets, the concept and tools provided by the NLF should be (re)used as far as possible in the area of voluntary cybersecurity certification.

In this model, market surveillance authorities in member states supervise the process, and exert ex-post control, which is proving a powerful system both in terms of conformity as well as for time to market.

In particular, this proves very effective for SMEs to demonstrate compliance and reach high quality levels in their products and services in an efficient and cost-effective way, putting them into a better position to compete with large enterprises or multi-national companies.

ETSI recommends that the NLF is used as a toolbox for the Cybersecurity Act and that the text is modified accordingly to include the clear sequence of *requirements – standards – certification* as well as self-assessment to determine conformity with specific requirements and standards.

---

[2] New Legislative Framework (Regulation (EC) 765/2008, Decision 768/2008/EC, Regulation (EC) 764/2008)

[3] Transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, development dimension. See "International standards and the WTO TBT Agreement: Improving governance for regulatory alignment", (https://www.wto.org/english/res_e/reser_e/ersd201306_e.pdf. Also rendered in Annex 2 of EU regulation 1025/2012 http://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32012R1025&from=EN

3. Rethink the three levels of security with a risk management approach and rethink the way objectives are described

Cybersecurity is not a one size fits all concept. Good security on a cheap IoT sensor is a very different concept from security on a large and sensitive electronic database. It is extremely difficult to define "levels" that are consistent across the broad range of security risks and the corresponding security controls used to address them.

The proposed Regulation identifies three assurance levels of European certification schemes: basic, substantial and high (Art. 46).

In a fast moving environment in which security is context-sensitive, certification outcomes should be easy to understand and meaningful in security terms. This suggests a risk management approach and levels that are defined within each context – guided by clear regulatory objectives.

Standardisation provides the mechanism to react with the appropriate flexibility to requirements within a risk management framework approach and to provide respective standards.

ETSI recommends that a risk management approach is adopted and that the definition of levels of assurance is left to market players.

With regards to the description of the objectives, Art. 45 of the proposed Regulation contains a set of objectives for certification schemes that is misleading:

- The set is partial and misses objectives that address some of the core issues of cybersecurity
- The objectives are too technical and as a result are likely to become obsolete rapidly
- Sets of objectives for cybersecurity standards need to be complete and coherent, such as the set found in ISO/IEC 27001 – an incomplete set is potentially damaging
- Objectives change over time as technology and the threat landscape evolve – standards have revision processes to deal with this. It is much more difficult to keep laws up to date.

ETSI recommends that Art 45 is replaced with a much higher level of objectives that avoid technical issues entirely, which are best left to standards to address.

4. Applicability and consistency with existing regimes

The proposed Regulation states that "the certification shall be voluntary, unless otherwise specified in Union Law" (Art. 48.2).

It should therefore be stated clearly that the certification framework should not apply for mandatory requirements in existing or future Union acts. Should there be mandatory requirements in Union acts, the NLF should apply. This does not exclude that the same standards that are used for voluntary certification may qualify for demonstrating compliance with mandatory requirements in Union acts and for giving a Supplier's Declaration of Conformity and operate under the Presumption of Conformity as laid down in Regulation 765/2008.

Similarly, national schemes for particular needs should not be excluded, neither should the use of SOG-IS or other regimes for national security or other related areas (noting that national security is not an EU competence in any case).

ETSI recommends that the text clarifies how the proposed system will interact with existing certifications schemes in other Union acts, e.g. TCAM and the Radio Equipment Directive 2014/53/EU, and how the migration path from current national or SOG-IS MRA certification schemes will be organized.

NOTE: There also needs to be an alignment with global developments in order to prevent segmented and expensive deviations from globally accepted concepts for European based industry.

5. Governance and processes

The proposed Regulation grants a substantially augmented role to ENISA, the "Cybersecurity Agency", but remains very vague about the processes and mechanisms to carry out its mission and interface with other bodies and agencies in EU and in Member States.

The proposed Regulation should clarify the processes by which ENISA will:

- Facilitate the establishment and take-up of European and international standards and other relevant global standards
- Liaise with standardisation bodies to ensure the appropriateness of standards used in approved schemes.
- Ensure a clear path by which industry and customers can give input to proposed certification schemes and also a path by which changes can be proposed by these stakeholders

Similarly, as per Art 44 of the proposed Regulation, only the Commission can request ENISA to produce certification frameworks. Member states in "the Group" (art 53) may propose to EC to request ENISA (to produce certification frameworks), but in any case the Commission is the gateway. Yet, the proposed Regulation leaves completely undocumented the "how" about this new Commission task: people, process, obligations of "the Commission", accountability.

ETSI recommends that the proposed Regulation further clarifies and specifies the processes and governance of these new missions granted to both ENISA and the European Commission.

Working with Standards Organizations in Europe

The European Standards Organizations - CEN, CENELEC and ETSI – have set up two formal standards groups that work with each other on cybersecurity: ETSI TC CYBER and CEN/CENELEC TC 13.

ETSI, with numerous security-focused technical committees and working groups, including TC CYBER, as well as its partnership projects 3GPP and oneM2M, continue to maintain an extensive array of activities for producing publicly available cybersecurity Standards, Specifications, and Technical Reports as well as organizing workshops, hackathons, and testing events.

In the case of ETSI, direct participation from members (whether large or small, public or for-profit sector) in technical committees at low cost facilitates broad participation in the standards making process. Much of this work takes place online and so facilitates easy access for all players.

ETSI's world class standards activity dashboards, as well as its open, searchable, freely available, and well-versioned publication with permanent URLs provide critically necessary availability to the industry and public at large.

As mentioned, a key consideration under the proposed Regulation are the standards which constitute the basis for certification. ETSI's work in this area should prove useful, including for:

- NIS Directive (work undertaken in cooperation with ENISA),

- Regulation (EU) No 910/2014 on "electronic identification and trust services for electronic transactions in the internal market",

- COM 2016/766 on "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility"

As well as for industry-led certification schemes[4].

[4] ETSI TR 103 456, *Implementation of the Network and Information Security (NIS) Directive*
http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf;
TC ESI publications to certify trust services and trust service providers in line with the eIDAS Regulation https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx;
ETSI standards developed by TC ITS WG5 (TS 103 097 , TS 102 941) are referenced in the Certificate Policy for the deployment and operation of European C-ITS https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf
3GPP Security Assurance Methodology (SECAM) (for network nodes) http://www.3gpp.org/news-events/3gpp-news/1569-secam_for_3gpp_nodes
Embedded UICC (eUICC) and the definition of test cases related to the support of multiple secure elements for mobile contactless communication