OFE Position Paper

Certification, Standards & Cybersecurity

February 2018

ofe

1. Introduction

OpenForum Europe (OFE) very much welcomes the ongoing debate about cybersecurity at the EU policy level. Cybersecurity is of utmost importance for digitisation, for the Digital Single Market and for the societal acceptance of digital transformations and the uptake of new technologies in general.

With the publication of a draft Cybersecurity Act[1], the European Commission recently provided a proposal for addressing the issue of trust in ICT technologies and systems by establishing a certification framework for Europe, with the objective of providing EU wide schemes against which cybersecurity will be assessed and respective information will be made publicly available.

OFE has been addressing this topic for some time now, and has run a task force on cybersecurity looking at standards and technologies as well as risk-based management approaches towards increasing awareness and driving the implementation of tech-neutral cybersecurity methods including in the context of policy objectives. While OFE welcomes the first part of the regulation, i.e., the articles that reconstitute the European Union Agency for Network and Information Security (ENISA), we have concerns about the approach taken in the second part (Article 42 onwards) which defines a regulatory framework for the cybersecurity certification of ICT products and services. This position paper therefore focuses on the latter part, i.e., the section dealing with the certification framework.

At its core, the European Commission's proposal for a Cybersecurity Act fails to place key emphasis on risk-based management, which is essential to effective cybersecurity practices and policy. Furthermore the proposal ignores the well-established practice of a clear separation of standards from conformity assessment and certification; it devalues standardisation and cybersecurity standards; it also ignores European Union principles under the New Legislative Framework, which provides a clean separation between legislation, standards, and conformity assessment. Cybersecurity schemes adopted under this proposal would conflate aspects of legislation, standardisation, and certification/conformity assessment.

[1] URL: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

With this in mind, OFE would like to offer the following thoughts and recommendations as input for further discussion and exchanges. We believe that the proposal has been put forward without sufficient discussion with stakeholders, especially without sufficient consultation of experts on cybersecurity standardisation, and without the benefit of the risk analysis which would be required before deciding on the best methods for further improving cybersecurity. There are a number of aspects which deserve further good in-depth analysis, including in what respect regulation may be a way to pursue and how standards fit into the context of cybersecurity certification and increasing trust.

2. Our reading of the Commission's proposal

In the proposal, the European Commission states that it intends to establish and preserve the trust and security of ICT products and services. To achieve this objective, the Commission proposes to introduce a legislative framework for the establishment of certification schemes, and to encourage the incorporation of security features in the early stages of technical design and development (security by design). National Certification Supervisory Authorities are supposed to monitor conformity assessment bodies and collectively advise the European Commission on certification schemes.

- The EC is entitled to create and approve cybersecurity certification scheme for any ICT products and services, whether for use by consumer, enterprises or governments.

- Each scheme can reference one or more standards and technical specifications, and can also define detailed requirements directly in the scheme itself.

- ENISA will prepare each scheme at the request of the EC, and the EC will adopt each scheme as an implementing act.

- ENISA is to consult relevant stakeholders in the development of any scheme, although this is not further elaborated.

- Equivalent existing Member State schemes for products and services will cease to be effective after an EU scheme is adopted, and Member States will not be able to create any new schemes with the same coverage as an approved EU Scheme.

- Each Member State must establish a National Certification Supervisory Authority to implement and supervise the Regulation. These will collectively form the European Cybersecurity Certification Group (ECCG), which may propose the creation of new schemes, whilst being limited to an advisory role in relation to the content and adoption of any scheme.

3. Concerns

OFE supports the Commission's overall goal of increasing trust. Our members, as developers and providers of innovative technologies, have a clear stake in improving trust, because it is a driver for market adoption. However, OFE has a number of high level concerns about the current proposal.

There is a lack of clarity about the scope and the processes behind the development of the certification schemes. It is not clear if the proposal covers all ICT products and services, or if it is focused on a particular sub-set. Considering the pervasiveness of ICT, the former interpretation is essentially an open-ended set. Deciding on which schemes to prioritize and pursue must be done in the context of a risk based approach.

There is also a lack of clarity in how a scheme's cybersecurity requirements will be established. Selecting existing standards or technical specifications from an array of choices can unintentionally disenfranchise communities; similarly, composing multiple standards into a scheme could have unintended consequences, including IPR issues. Selection of standards and composing them into products is typically a core competence of vendors, and is vital to a competitive marketplace. Additionally, Member States may already have established preferences for different standards, and thus need to be directly involved in reconciling them.

- The scope of this proposal is not clear - potentially, it could cover all ICT products or services. This means that it is not possible to know whether or not a product currently being developed will need to be certified. In this regard, it's possible that the Commission may have a priority list, but if so, so far at least this is not publicly known. The community would benefit from a roadmap.

- According to the proposal the Commission would have a lead role in deciding what schemes are needed and when, what products and services should be covered by a scheme, and what standards and requirements have to be complied with for certification. Moreover, the Commission would be the only body in the EU that can approve an EU-wide certification scheme. Member States are only formally involved via the advisory European Cybersecurity Certification Group. There is no formal involvement of the European Standards Organisations (CEN, CENLEC, and ETSI), of National Standards Bodies, of societal stakeholders, or of industry.

- Standards and technical specifications are only considered optional for defining the requirements of a certification scheme, and requirements are allowed to be created and directly included in a scheme itself. There are no defined rules in the proposal, and thus it would be possible to directly develop requirements, even if suitable standards already exist. This devalues the achievements and potential of standardisation. Instead of putting community-approved, international and European cybersecurity standards into the centre of the assessment of the cybersecurity of products and services, uncertainty is created by separating standards that are openly available for everyone for implementation from "pseudo-standards" directly expressed as requirements in certification schemes. This is bound to lead to confusion in the marketplace, and may also impact the implementation of cybersecurity standards and hamper the development of new technologies and techniques around cybersecurity and thus stifle innovation.

- Moreover, although a scheme may initially be voluntary, it could become de-facto mandatory "by the back-door" if an EU Member State were allowed to give preferential treatment in procurement situations to those products and services that comply with an EU scheme. In fact, on several occasions the Commission has admitted that a scheme could become mandatory at a later time it is not clear if revisions to the scheme would be permitted. As an aside, the whole notion of versioning of a scheme is completely missed in this proposal.

Selecting and composing standards - as opposed to defining essential requirements - creates a new practice which is essentially at odds with the New Legislative Framework and the European Standardisation System and creates a parallel system. The proposal devalues consensus-based standardisation and permits cybersecurity standards to be ignored. In the absence of defined open and transparent processes that permit industry and other stakeholders to be formally involved, such as those provided by standardisation bodies, there is a huge risk that cybersecurity requirements will have no industry support, not be practical, and appear to be imposed. Moreover, by creating a system in parallel to cybersecurity standards there is a risk that uncertainty will be created in the market place which hampers adoption of technologies rather than increasing trust. Without additional structures in place, there is also a risk that a scheme may not have adequate IPR protection, especially related to Standards Essential Patents with respect to any detailed specifications made directly within a scheme. Another example of a lack of clarity in these proposals is that while labelling has been removed from the title of this draft regulation, schemes would be permitted to define the conditions under which a mark and label may be used, although no scoping of such terms and conditions is defined.

Regarding the voluntary nature of certification schemes, we are concerned that a scheme could become de-facto mandatory either because the scheme is in support of existing legislation, such as the NIS directive or GDPR, or in cases where a Member State gives preference to a scheme during procurement. Such a situation would, once again, lead to a lack of clarity and confusion in the market place. In order to avoid such a situation an in-depth discussion should be held as to what extent there might be cybersecurity requirements that are essential in a similar way to market access requirements in the context of the NLF, and to what extent harmonised European Norms could be used for complying with these requirements, including a respective declaration of compliance and presumption of conformity.

4. Way forward

Industry has a strong preference for relying on foreseeable market-driven, consensus-based standards (and any associated certifications) as well as for reinforcing the risk management approach enshrined in the NIS directive. The proposed Act not only risks disrupting the current framework but builds a parallel system without improving the effectiveness. While one EU-wide cybersecurity certification scheme is better than the existing patchwork of national solutions, the current formulation of the proposal lacks clarity in many ways (see point 3) and ignores the well-established European regulatory framework.

- We agree that if there are to be proposals dealing with certification, it would be preferable to have a single EU-wide cyber security certification/standard, rather than a patchwork of national solutions; however, we have concerns about establishing a new process framework to achieve this. EU Regulation 1025/2012 on European standardisation already provides a mechanism which can establish EU-wide schemes and standards.

- If the proposed framework is the way forward, the development of a scheme needs to follow open and transparent processes that permit stakeholder engagement at all stages, and must that take into account standards essential patent issues that may arise when defining the requirements of a certification scheme.

- It is also necessary to clarify whether the scheme is to be fully or partially voluntary, whether this will be the rule in the future, and what processes are intended to be used in the future should it be desired to make a certification scheme mandatory.

To increase the quality of the proposal, we suggest that existing or additional structures could be further considered. Indeed, proven existing EU structures are already in place that can achieve the same objectives of the proposal, namely the New Legislative Framework (NLF), and Regulation 1025/2012[2] on European Standardisation, which enables and uses market-driven standards and provides room for regular innovation.

However, if the new framework is the way forward, at least this framework should explicitly define open and transparent processes that permit and encourage stakeholder participation, and address the IPR issues that standards bodies have to deal with. Addressing these issues should ensure adherence to the World Trade Organization Agreement on Technical Barriers to Trade.

Finally, it may be worth noting that the regulatory measures taken in Europe should be made in such a way that they can be recommended and replicated in other areas world-wide. The ICT industry is ready to support the European Commission and the legislators in this in a broad and in-depth dialogue that is urgently required. International and European standards are a reference point that have global impact and can be promoted globally.

[1] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF

We wish to reiterate the need for further and on-going discussion and analysis of the proposal, with a particular need to focus attention on furthering voluntary adoption of a 'risk-based management' model. Indeed, significant caution should be used with respect to the decision whether certification should be mandatory (whether *de facto* or *de jure*), and whether prescriptive regulation – and if so, in what respect – can better secure European citizens and organisations.

For more information, please contact OFE's CEO Sachiko Muto at sachiko@openforumeurope.org.

OpenForum Europe (OFE) is a not-for-profit, independent European based think tank which focuses on openness within the IT sector. We draw our support not only from some of the most influential global industry players, but most importantly from across European SMEs and consumer organisations and the open community. OFE also hosts a global network of OpenForum Academy Fellows, each contributing significant innovative thought leadership on core topics. Views expressed by OFE do not necessarily reflect those held by all its supporters.

OFE Limited, a private company
with liability limited by guarantee
Registered in England and Wales with
number 05493935

Registered office: Claremont House,
1 Blunt Road, South Croydon, Surrey
CR2 7PA, UK