DIGITALEUROPE

DIGITALEUROPE's position paper on the European Commission's proposal for a European framework for cybersecurity certification scheme for ICT products and services

Brussels, 15 December 2017

INTRODUCTION

With an increasing number of online activities and services, the digitisation of the industry and rising number of connected devices (the Internet of Things), the role of cybersecurity has become even more crucial to provide a stable digital economy and ensure the trust of consumers. For DIGITALEUROPE, ensuring cybersecurity, from critical infrastructures to consumer devices is an imperative. It, therefore, requires the appropriate measures to tackle cyber risks that can compromise the functioning of our economy and society.

Following the growing number of harmful cyber-attacks, cyber security and resilience of the European Union have become a public policy priority of the European Commission, which adopted on 13 September 2017 new legislative measures on cybersecurity. The main piece of legislation consists of a draft regulation - "the Cybersecurity Act"- based on two pillars: (1) the revised mandate and responsibilities of the European Agency for Network and Information Security (ENISA); (2) a European framework for Certification Schemes for ICT products and services.

The second pillar of the proposed Regulation is of particular importance to DIGITALEUROPE, which had already expressed its views on cybersecurity certification and labelling schemes in March 2017[1]. The proposed framework for cybersecurity certification plans to empower the European Commission to adopt EU-wide certification schemes for ICT products and services.

DIGITALEUROPE welcomes the main objective of creating a harmonised EU market for cybersecurity certification schemes. However, we believe that the proposal put forward by the European Commission could be improved to guarantee higher participation and involvement of the industry and rely on market-adopted global cybersecurity standards. Therefore, we recommend the following improvements to be taken into account in the ongoing law-making process.

We are ready to participate in a constructive debate and provide valuable industry knowledge to support policy makers in their work.

[1] DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes, 23 March 2017

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

DIGITALEUROPE'S POLICY RECOMMENDATIONS

DIGITALEUROPE calls on European policy-makers to:

- **Strengthen and streamline the voluntary aspect of European certification scheme by making the regulatory proposal an "enabler" of certification schemes' mutual recognition** in the EU for those companies which freely chose to certificate based on their business strategies;

- **Adopt an EU framework that allows self-certification as a principle** and as the default, and only require third-party certification for critical requirements.

- Provide additional guarantees that **existing certifications under current certification schemes will be granted fair terms of renewal and mutual recognition**;

- Include provisions to ensure the framework is **complementary to existing frameworks and international mutual recognition schemes** as opposed to competitive;

- **Clarify the scope of the certification** by providing a precise definition of ICT products, processes, and services that could be subject to certification scheme as well as the assurance levels and **involve industry in this process**;

- Increase **transparency and openness of the elaboration and adoption of EU cybersecurity schemes**, especially by:
    - Allowing **industry to request the elaboration of a candidate scheme** - under certain conditions;
    - Closely **involving industry in the drafting of candidate schemes**, especially in the standard(s) reference use.

- **Adapt the security objectives** so that they better reflect the range of security certifications that will come under the EU framework;

- **Use existing global standards in requirements that certification will be assessing against** and consider sector-specific standards. Global standards shall remain the key reference to certification process in Europe;

- **Ensure continuous compliance and enforcement**, to guarantee trust, security and a proper functioning of the European Single Market.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

DIGITALEUROPE'S VIEWS ON MAIN ELEMENTS OF THE REGULATION

1. Support to the general principle to create an EU market for cybersecurity certification

European approach: DIGITALEUROPE shares the goal of addressing the current fragmentation and complexity of certification schemes across the EU and create a more integrated EU Digital market for cybersecurity, which is very welcomed by industry and consumers. The multiplication of ICT security certification schemes at a national level in the EU has not only led to administrative, timing and cost issues but also to the complexity of managing multiple non-aligned or non-standardised schemes that do not benefit from mutual recognition. In principle, the objective of a single certification process in one Member State, which is automatically recognised across all Member States, would have benefits for the industry including on both competitiveness and a significant reduction of costs of certification and time to market. We also believe that reference to standards should be based in a first place on global standards to recognise the global nature of the industry.

Security by design: DIGITALEUROPE supports the fact that a "security by design" approach is promoted and specifically identified in the proposal of the European Commission. To further secure ICT products, they should be designed with cybersecurity in mind, from the earliest phase of product or system development. The features of ICT products must be adapted to the risks that are linked to the product capabilities and usages. DIGITALEUROPE also believes that the "security by design" approach should be based on global standards.

Enabling and encouraging innovation: it is imperative to ensure that any certification scheme is open to new technological approaches, solutions, and innovation. It remains still unclear how this could be possible in the current proposal of the European Commission, to guarantee adaptation to future digital developments. Adverse effects on small and medium-sized enterprises (SMEs) of the European certification framework must be thoroughly assessed. SMEs may be not able to afford another level of certification and secondly will have concerns in short product cycles about their intellectual property rights, whether this be trade secrets, copyright or patents, since a quasi-mandatory approach would entail third-party certification.

2. Voluntary approach and self-certification must retain a key role

Keep a voluntary EU Framework: DIGITALEUROPE supports the voluntary approach taken by the European Commission. However, one key concern is that it is likely that the adopted European schemes will become de-facto mandatory, for the following reasons:

- EU schemes will prevail over national existing ones, that must be removed (article 49). The obligation of using one certification scheme, to the detriment of other possible schemes that will have to cease to exist, goes against the principle of a voluntary approach. It is also problematic where existing schemes are part of standards that have broader application than the EU alone;

- A Member State can decide to give preferential treatment in a tender to products and services complying with a European scheme;
- The draft regulation stipulates that a European cybersecurity certification scheme will be voluntary, "unless otherwise provided in Union or national legislation" (Recital 57 and article 48 paragraph 2).

Self-certification, has to be included in this regulation and should be the default. Third-party certification should only be required after careful consultation and only in areas necessitating high-level security requirements, such as in critical infrastructure.

Self-certification, i.e. self-declaration without the involvement of a third party, is a recognised and tested approach used by vendors, for which the industry has extensive experience, and is supported by EU lawmakers in market access legislation. It responds to the need for flexibility, agility, manpower, and limits on costs that must be borne by vendors when certifying. Self-certification must, therefore, be a recognised principle, of which third-party certification shall be an exception for critical requirements. As regards third-party certification, the laboratories that will test any critical product should be recognised at a European level after an assessment by a peer external party (accredited body). Consequently, as currently drafted, the European cybersecurity scheme does not allow the possibility for self-certification and should be modified.

3. Relation and compatibility with existing certification schemes

Mutual recognition of existing certifications: several cybersecurity certification schemes – at an international or national level, already exist and are used by the industry. The draft regulation doesn't address the question of existing certifications delivered according to these schemes and should, therefore, be tackled. We recommend that the proposal includes provisions to ensure that currently certified products can benefit from mutual recognition within the EU, provided they meet specific requirements to be set and then assessed by ENISA, with the involvement of the industry. As regards existing international mechanisms, the proposal should ensure that EU adopted schemes are both compatible with international mutual recognition arrangements and aim to join them where possible.

Concerning existing national certifications, the proposed framework provides for a transition period for certifications issued in accordance with national schemes that are set to be replaced by European ones. Such certificates will remain valid until their expiry. Given that such certifications are often subject to maintenance processes whereby they are adapted to account for minor updates, we would welcome clarification that such adaptations are not considered to invalidate the certification.

Moreover, when companies upgrade their products and make significant changes to security features or architecture, they may seek recertification. They may also seek to recertify a product on the same basis after the original certification expires. While we would not expect that they can do the new certification under the old scheme, we would nonetheless welcome a clarification that the previous documentation could serve in the new scheme as the baseline against which new changes are compared.

4. The need for a clearer definition of the scope of the proposal

At this stage, the article 2 **definition of "ICT products and services" is extremely vague** and provisions are unclear on how each scheme will be defined in terms of product or service that it will cover (article 43 & 47 (a)). An "ICT product and service" under Article 2(11) is defined as "any element or group of elements of network and information systems". This indicates that security certifications that address specific assets, or products, will be covered but it does not seem to cover services, insofar as services are intangible and cannot be fundamentally equated to the assets on which they are delivered.

In addition, **Article 43 mentions a broader scope: "products, processes, services and systems"** and footnote 8 of the explanatory memorandum also references processes. As regards processes, certifications that focus on how the company adopts processes to protect data (such as ISO 27001), manage vulnerabilities (such as ISO 30111) or develop securely industrial product (IEC 62443 4-1 Secure development life-cycle requirement, or ISO 27034, for example) could be covered.

The proposal to have **three levels of assurance** basic, substantial, and/or high (in article 46) reflects the necessity to adapt the scheme per type of product or service and related cybersecurity risks. First, DIGITALEUROPE finds misleading to define "basic" with a limited degree of confidence, because it would not help build the trust of users. Basic should be translated into an achievement of minimum requirements to consider the product secure, in its product functionality as well as its potential to be hijacked to provide damages for the network and other services/devices. According to the type of ICT product and its use, cybersecurity risks and requirements would not the same, if that ICT product was used for instance as a component for a critical infrastructure or for a consumer good. Additional clarification is needed on how these three levels will interplay in a given scheme and how a vendor could decide to choose one or several assurance levels, depending on the use case of the same product.

5. Adapting provisions relating to security objectives

It should be reinforced that the security objectives identified under Article 45 are neither exhaustive (in other words, a certification scheme may include additional security objectives) nor should it be necessary to meet them all in order to qualify. The framework is trying to cover a wide range of certifications and types of devices and services and these may not easily boil down to one set of objectives. In general, it is better to **set the overarching goal as opposed to prescribing** how to get there – which is the realm of the certifications themselves.

Certain of the objectives do not seem to sit very well with product requirements. For example, 45(f) is an objective to restore availability – which is largely the domain of the entity operating the devices rather than the device itself.

45(d) and (e) also presume ongoing management of products in their operational environment, which is not something under the control of the device manufacturer. It is also unclear that recording which data, functions, and services have been communicated under point (d) serves a security purpose. The

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

more general objective in (d) and (e) seems to have the ability to generate log data, to the extent this is necessary for security purposes.

45(g) requires that ICT products and services are provided with software that does not include known vulnerabilities. It is not unusual, however, for products to be shipped with vulnerabilities that do not represent a specific risk in their common operational environment. In other words, the product may only need to be resistant to attacks performed to a particular level of sophistication and one needs to assess the attack vector needed to take advantage of the vulnerability. As such, this security objective would be better worded as a requirement to assess vulnerabilities.

6. Expanding industry involvement and participation in the preparation of certification schemes

The **engagement of the industry in cybersecurity policy and potential impactful measures is of crucial importance** for the ICT market. DIGITALEUROPE has repeatedly called for considering not only the usual top-down approaches, but to include bottom-up approaches that aim at enhancing private sector cybersecurity. However, the proposed European Framework for certification scheme rather supports a traditional top-down approach to elaborate cybersecurity certification schemes.

In order to effectively transfer the preparation of cybersecurity certification schemes, there also needs to be a transfer of resources, in terms of manpower, expertise, budget, and facilities. This cannot be borne by ENISA alone. This framework will only be able to scale if existing resources for certification activities maintain a major role in the preparation of candidate schemes.

Additionally, the **involvement of the industry in the current provisions is very limited and must be expanded**. For instance, in the proposal a candidate scheme can only be elaborated at the request of either the European Commission, a Member State or the European Cybersecurity Certification Group (in article 44). "All relevant stakeholders shall" be consulted by ENISA but are not necessarily entitled to provide their expertise or assistance for the preparation of candidate scheme, nor there is an avenue for them to propose candidate schemes to the Commission. The industry as well as standardisation organisations must be allowed to be involved in the drafting and preparation of candidate schemes, through a consultation process in order to provide expertise to ensure the design of efficient certification schemes.

7. Global standards must be at the core of the framework and in all certification schemes

Standards are at the heart of ICT products and services - including Industrial Automation Control Systems (IACS) and IoT devices. This includes standards produced by formal Standard Development Organisations (SDOs), such as the International Standardisation Organisation (ISO) and the International Electrotechnical Commission (IEC); by European standards organisations, such as CEN/CENELEC and the European Telecommunications Standard Institute (ETSI); and by globally recognised fora/consortia. These SDOs and consortia have produced cybersecurity standards for ICT

and ICT infrastructure, products, hardware, and software, that are already being used internationally by industry.

In the draft proposal of the European Commission, there are vague references to standards: it is key that **requirements of certification schemes refer to global standards** both to avoid a fragmentation of a market that is global and for competitiveness purposes. Only in the case that there are not any internationally recognised standards published should the ESOs develop homegrown European standards. Requirements and technical details should not be directly embodied in a scheme itself and should only be done by reference to standards. It is also of crucial importance to adopt a sector-specific approach that refers to sectorial global industry standards[2].

Additionally, when preparing a scheme, it should not be up to ENISA to freely decide which standard(s) to specify, but to assess the suitability of the standards on which the certification schemes are proposed to be based or refer, with the support of the industry. The process of elaboration and adoption of certification schemes should also allow the involvement of SDOs.

8. Continuous compliance and enforcement

There are several provisions that presume a continuous compliance approach in the framework, including Article 47.1(g), 47.1(j) and Article 48.6. This fails to recognise certifications that amount to the assessment of a specific product at a particular point in time.

The limitation of the applicability of certifications to a maximum of three years under Article 48.6 is particularly problematic. Given that existing product assurance certifications can take 12 to 18 months to achieve, and that they reflect security at a point in time for a specific version of a product, it is not clear why there should be an expiration date.

National certification supervisory authorities are given the power to audit holders of certifications under Article 50. It is more common, however, for the supervisory authorities to choose to assert their authority through powers to assess the capabilities of conformity assessment bodies, who may, in turn have powers to audit the certification holders, if applicable. It would be better, therefore, to express this in more flexible terms such that the **supervisory authorities have ultimately authority for ensuring effective compliance and countering misuse of certifications**.

We also take issue with the requirement on supervisory authorities to share information with other authorities on non-compliance of ICT products and services with certification schemes. If a vendor fails to meet the requirements to certify against a specific scheme, for example, sharing information about the failure and reasons why amounts to the sharing of business confidential information without authorisation.

[2] E.g. ISO-SAE 21434 for road vehicles - Cybersecurity Engineering standard - or IEC 62443 series for Industrial Control Systems

--
For more information please contact:
Iva Tasheva, DIGITALEUROPE's Policy Manager
+32 2 609 53 10 or iva.tasheva@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 62 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK