DIGITALEUROPE

DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes

Brussels, 23 March 2017

EXECUTIVE SUMMARY

DIGITALEUROPE as the voice of the digital technology industry in Europe welcomes the opportunity to comment on the European Commission's on-going work within the field of cybersecurity, particularly the potential role for cybersecurity certification and labelling schemes for ICT products. DIGITALEUROPE is concerned that the potential future proposals of the European Commission in the field of cybersecurity certification and labelling **may be focusing on the wrong policy priorities**.

DIGITALEUROPE wishes to emphasise that today we already have mature frameworks to support higher security environments as well as lighter self-assessment approaches that serve dynamic emerging markets. The European Commission should not look to establishing new frameworks as they typically take decades to be developed and adopted. Instead, the two current approaches need to be developed further for greater efficiency and agility. Time consuming and expensive certifications work for the governmental and critical infrastructure sectors, but cannot be applied to the dynamic world of consumer products with short life spans or multiple contexts of use. Therefore, DIGITALEUROPE believes any future actions by policy makers in the field of cybersecurity certification and labelling should take into consideration the following criteria:

- **Cybersecurity is a global issue and requires international solutions** – Cyber attacks know no borders and therefore standards and related certifications play a significant role in creating a safer ICT environment. Any future EU activity in the field of cybersecurity standards, certifications and labels should take into due account the existing international ecosystem.
- **Flexible cybersecurity solutions** - To stay ahead of malicious attackers, industry must be able to develop and deploy new tools to protect our digital economy against changing cyber risks. Policymakers should make sure that any regulatory action in this field keeps abreast of state-of-the-art technology.
- **One size does not fit all in a complex cyberspace** - A new EU certification framework would not be able to cover a broad set of products/services as the nature of products and services as well as the magnitude of cybersecurity risk vary significantly.
- **Promoting consumer protection and innovation** - Component/product labelling could potentially lead to a false sense of security for end-users in the consumer market. Benchmarking cybersecurity practices, on the contrary, would allow both consumers and organisations to compare situations and form an idea of the cybersecurity state-of-the-art.
- **Certification and competitiveness** – Regulated certifications and security evaluation involve considerable costs. It is important that it remains voluntary and that a range of agile self-certification mechanisms are allowed to flourish according to the market at hand. It is important not to erect market barriers to smaller companies by mandating high entry costs.

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

EU CYBERSECURITY MATTERS

With an increasing number of activities and services offered online and the proliferation of connected devices (the 'Internet of Things'), it has become more evident that cybersecurity plays a crucial role in ensuring the correct functioning of our digital economy. Appropriately securing network and information systems, from critical infrastructure to consumer devices, is the only way forward. Cyber threats do not only pose a serious risk to individuals, businesses, and public administrations but also to the very fabric of contemporary society.

The European Commission acknowledged cybersecurity as a fundamental policy priority in its first **European Cyber Security Strategy** (2013) for an open, safe and secure cyberspace. The **Network and Information Security (NIS) Directive** (2016) is the first cross-sectoral legislation aiming to improve cooperation among Member States and to harmonise security and notification requirements for operators in key sectors. In its **Digital Single Market Strategy** (2015), the European Commission has launched a **Cyber Public Private Partnership (cPPP)** to stimulate the EU cybersecurity industry through its Horizon 2020 programme and investments by market players.

RECENT EU PROPOSALS ON CYBERSECURITY CERTIFICATION AND LABELLING

In the course of 2016 the European Commission announced two initiatives for further assessment in the field of certification and labelling: 1) a security **certification framework for ICT products** and 2) a **"Trusted IoT label"** giving information about different levels of privacy and security and, where relevant, demonstrating compliance with the NIS Directive.

1. Security Certification Framework

The concept of a security certification framework for ICT products and services was raised in the European Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[1] and the accompanying staff working document[2].

The staff working document pointed out that **market inefficiencies could arise with regulated certification schemes**, particularly for national schemes that define standards and evaluation methodology nationally and only recognise certification bodies within their own territory. Moreover, the European Commission notes that market fragmentation and restrictions to trade can be overcome by making use of European or international standards and agreeing common security requirements to the maximum extent possible, as well as highlighting the value of mutual recognition agreements. Of the four example schemes mentioned in the Annex, two are international mutual recognition agreements (CCRA and SOG-IS) and two are national schemes (CPA in the UK and CSPN in France[3]).

Common Criteria is an international standard (ISO/IEC 15408) that enables users to define their security functional and assurance requirements through Protection Profiles, against which vendors can make claims about their products and have them independently evaluated by testing laboratories. The Common Criteria Recognition

[1] COM(2016) 410 final https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

[2] SWD(2016) 216 final https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-cppp-and-accompanying-measures

[3] Commercial Product Assurance (UK) and Certification Sécuritaire de Premier Nouveau (France).

Arrangement ("CCRA") is an international agreement between national certification bodies that mutually recognises evaluation results from laboratories in different jurisdictions.

However, the recent adoption of a different approach for Common Criteria – moving away from Evaluation Assurance Levels ("EALs") in 2011-12 and renewing CCRA in 2014 - led to a transitional period where diverse requirements for Common Criteria certification in different EU/Asia Pacific jurisdictions and the US/Canada, necessitated multiple regional certifications for one product. This situation illustrates that, even if a pan-European approach is achieved, global support is required to render CCRA as effective as it was in the past. **Harmonising only within Europe, or beginning the framework anew, will continue to hurt European companies and efforts should be directed to strengthening the global approach.**

SOG-IS, on the other hand, is a European group that coordinates the development of Common Criteria protection profiles and looks to agree a common European position within the CCRA group. The SOG-IS Mutual Recognition Agreement ("MRA") allows recognition of common criteria certificates up to EAL. With regard to SOG-IS, higher level security requirements typically reflect the views of host governments and specific sectors, and therefore should be considered separately.

National schemes exist primarily to offer a cheaper and faster alternative to participating entities, which streamline requirements to those necessary for the national market in question. Such schemes only become a hindrance if they are given preferential treatment in the market. To the extent that international certifications remain equally valid and compatible in, for example, public or critical infrastructure procurement, then they may have a niche role to play.

The European Commission's Communication itself addresses a broader set of ambitions for the certification framework. It states that a possible framework should 1) cover a wide range of products, 2) apply in all 28 Member States and 3) address any cyber level.

Common Criteria and the existing international mutual recognition schemes for ICT product certification cannot be the answer to all three of these ambitions. Such certifications typically tend to focus on either government or critical infrastructure use cases. As such, they focus on sectors where the cyber risk is highest. Independent product evaluation is very resource-heavy and there are also other evaluation frameworks based on the idea of SDL (Security Development Lifecycle), such as software-based ISO/IEC 27034 as well as certifications applicable to specific types of systems including ISA/IEC 62443. The process-based approach to certification is an important element of the big picture that needs to be included. Moreover, given continued contraction of product development cycles and life spans, **certifications such as Common Criteria will not be able to serve the majority of ICT product**s. At the same time, creating an overlay in terms of a new EU ICT product security certification framework that ends up increasing the cost if it is required on top of the existing certification, or weakens international harmonisation if it tries to replace it, is not a viable solution either.

Therefore, agile self-assessment schemes and test automation environments will need to be created and evolved to ensure ICT products have minimum security capability appropriate for a context where they are used. While Common Criteria cover critical infrastructure/government across a range of international countries, self-assessment allows a wider range of products to be addressed across non-critical environments.

To the extent the European Commission has a role to play on ICT product security certifications, it should evaluate whether preferential treatment is being given in procurement to national schemes and **favour an equitable approach with international protocols that promote the use of agile self-assessment schemes and test automation environments.**

2. Trusted IoT Label

In its July 2016 Communication, the European Commission also brought forward the idea of a European label for trust/security of ICT products. This has since been further elaborated in policy discussions in the context of the Internet of Things ("IoT") and has been suggested as a potential item for a Trust in the Digital Single Market package in the Spring 2017.

In the Communication, the label discussion is held as an extension of the product certification discussion. It is worth, however, **distinguishing between the two**. As noted above, ICT product security assurance certification schemes tend to focus on the critical infrastructure and government section of the market. Labelling, on the other hand, suggests the consumer market – providing quick-to-digest, transparent information to a consumer at the point of sale as opposed to demonstrating characteristics in more sophisticated business-to-business transactions.

This difference in characteristics means that the **products themselves are highly unlikely to have the same level of security functionality** (with good reason as their use case is likely to be lower risk) and that the buyers are less likely to support the cost premium attached to extensive and independent evaluation for the vast array of products on the market. A 'light-touch' label, on the other hand, is likely to run into its own problems.

A contrast is often made to energy-efficiency labelling, but there are some important differences. Firstly, while energy use can be subject to fairly homogenous or limited measurements (e.g. KwH), security is not as homogenous. What matters for one set of products does not necessarily matter for others. This is reflected in the critical infrastructure space with Protection Profiles under the Common Criteria, but this would be more difficult to reflect on a single simple label for consumers, or across the vast range of products considered within the sphere of IoT.

Secondly, and most importantly, **security is not static**. While a product may achieve a top rating at the point it is put on the market, six months down the line changes in the threat landscape may **render it insecure**. While users of ICT products in the critical infrastructure sector or other sensitive settings are likely to have means to keep up with developments across the lifecycle of a product, at the consumer end of the market, there is an imbalance of information and the devices do not even necessarily have update capabilities. **Labelling, therefore, creates the very real risk of a false sense of security.**

DIGITALEUROPE has already submitted comments to the European Commission on the value for such a scheme on a mandatory basis. We continue to express an openness to the concept of a **voluntary IoT Trust Charter** – allowing the industry ecosystem to sign up to a set of principles that elucidate their approach to security and privacy.

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

INFORMATION SECURITY CERTIFICATION

ICT product assurance and ICT product labelling are not the only types of certifications in the cybersecurity arena. The EU has recently successfully adopted the NIS Directive, introducing technical and organisational security requirements for a number of sectors. In many cases these are likely to be implemented by the use of information security controls and processes, and standards that are set out to define them. Certification against information security standards differs from product certification/labelling as described above insofar as it is **not the security of the product itself that is being evaluated but the processes and controls established by the organisation** in question such that they protect the data of the user under their control or remit. DIGITALEUROPE encourages policy makers to adopt a **harmonised approach to such security measures** and the means for their implementation, as well as to rely on the existing mature international framework on information security.

PRINCIPLES

Given the range of initiatives and implementation activities relating to security certification, labelling and standards, we would like to set out a number of principles that we believe can help guide policy makers in their endeavours:

1. Cybersecurity is a global issue and requires international solutions

Standards are at the heart of ICT products and services. International standardisation bodies - such as the International Standardisation Organisation (ISO), the International Electrotechnical Commission (IEC), the World Wide Web Consortium (W3C), the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standard Institute (ETSI) - have produced cybersecurity standards for IT infrastructure, products, hardware, and software.

Cyberattacks know no borders and therefore global standards and related certifications play an even more significant role in guaranteeing the cybersecurity of networks and devices. Any future EU activity in the field of cybersecurity standards, certifications and labels should take into due account existing international regimes. New regional or national certification schemes are recognised as a right of a nation, however they do not only carry a risk of introducing trade barriers, but would actually **increase security risks unless they remain aligned with international standards and certifications**. Differences with existing international standards may create overlaps and, more dangerously, misrepresent the security of an offer, leaving gaps for consumers and businesses, leading to possible further vulnerabilities in their systems. In fact, only a rigorous assessment of the eventual gaps could justify a move towards new schemes without undermining the global ecosystem's resilience.

At a European level, the European Network and Information Security Agency (ENISA) has carried out an extensive mapping of international standards and European certification schemes in cloud and digital service provider security, which should form the basis of further analysis by the European Commission and the European Cyber Security Organisation (ECSO)[4]. Any EU certification framework should rely on existing standards to be able to **scale across borders**, ensuring global consistency and broad market adoption.

For a certification to be meaningful, it must be based on an industry standard that creates a uniform, comparable, practicable and technically proven foundation. In view of the strong export orientation of European companies,

[4] ECSO is the industry-led contractual counterpart to the European Commission for the implementation of the cPPP (https://www.ecs-org.eu/about)

international standards should form the basis. Mature, internationally recognised certifications in product assurance and information security are already readily available, whereas the transaction costs and uncertainties would be significantly greater for a new framework, particularly if it is not international.

2. Only flexible cybersecurity solutions can address fast-developing technology and ever- changing cyber threats

As the threat landscape becomes more sophisticated, the effectiveness of regulatory responses depends on awareness and the agility to adapt to changes. Security is a dynamic concept: networks, computers, electronic devices, programmes and data can be considered secure today thanks to the defence techniques developed by industry. Cybersecurity is becoming central across the board in IoT devices and will serve as a distinguishing feature. An excessively narrow and static certification or labelling systems may actually **restrict the range of security solutions**, particularly if it outlines the requirements and implementation measures. This prevents innovation and market diversity.

To stay ahead of malicious attackers, **industry must be able to invent, develop and deploy new tools to protect our digital economy against ever-changing cyber risks**. To support this much-needed activity, governments and policymakers should make sure that any regulatory action in this field ideally keeps abreast of state-of-the-art technology and at a minimum allows enough flexibility for the cybersecurity industry to adopt the most appropriate solutions and technology without falling out of compliance with regulations.

DIGITALEUROPE fully supports industry engagement by the EU Institutions in defining future cybersecurity scenarios in the EU. However, we consider that along with traditional top-down approaches in regulating cyberspace, EU policymakers should look also at **bottom-up approaches** to enhance private sector cybersecurity. Cybersecurity strategies in UK, US, Italy and Japan reflect the trend of emphasising private sector self-governance over top-down direct regulation.

As an example, the UK's Cyber Essentials programme defined requirements involving self-certification for basic cyber hygiene practices for enterprises. In the US, the NIST[5] Cyber Security Framework mapped industry-recognised cybersecurity practices and indicated the activities to achieve specific outcomes in risk management. **Self-certification or self-assessment schemes** (such as the GSMA's IoT Security self-assessment framework) could address in a more rapid manner the need for harmonised solutions, and, at the same time, these could evolve according to the pace of technology and its use case development. On the contrary, **regulated certifications and labels may not pass the test of time** in the future cyber threats landscape. Using self-declarations, companies can demonstrate in a transparent and comparable manner how they have considered cybersecurity in their products and solutions. This enables a more differentiated statement to be made to the customer regarding the security of a product than a generalised label, instead of running the risk of conveying a false conclusion regarding the security of a product to the customer.

[5] US National Institute for Standards and Technology (NIST)

3. One size does not fit all in a complex cyberspace

A new EU certification framework would not be able to cover situations which are very different in **nature and magnitude of cybersecurity risk**. While users in the critical infrastructure or government sectors may require certain assurances and independent evaluation, the same may not be true of an everyday consumer device. Ensuring resilience for a consumer device or a critical infrastructure entail different practices and expectations. Some verticals in an IoT ecosystem (e-health, smart agriculture, industrial automation) may expose individuals and businesses to distinct threats and consequences. Existing certification schemes (e.g. EU energy labelling) cannot apply by analogy to cybersecurity, which is not as measurable and immutable as energy performance, as it is determined by the data in question, the likelihood of malicious activity and the ability to exploit. Similar labels ("A++ secure") would only represent an incentive for malicious actors to hack a device or compromise a service.

In view of ensuring a harmonised approach in the EU, DIGITALEUROPE considers the identification of **common cybersecurity baselines** as a crucial first step. In particular, instead of focusing on products or services, we deem it more important to look at **processes**, with a common set of guidelines for levels of security and related requirements, which ensure the necessary cybersecurity for users, public administrations and businesses. In favouring **security-by-design** processes, we would be able to promote capabilities to cope with cyber risks and a faster adoption of industry best practices instead of imposing technologies.

4. Self-assessment schemes enable consumer protection and innovation

In the context of an enhanced European Cyber Security Strategy aiming at raising levels of awareness and preparedness in all Member States across a range of common use case scenarios, voluntary and bottom-up cybersecurity schemes would better match these expectations. Mutual recognition with non-EU Member States would be made easier by anchoring EU schemes to international standards.

Benchmarking cybersecurity practices would allow both consumers and organisations to compare situations and form an idea of the cybersecurity state-of-the-art. Administrative costs related to certifications and accreditation bodies would not be at the final users' expense nor represent an additional cost to go to market for innovative SMEs. Market dynamics would reward reliable operators offering solid security-by-design processes and transparent **self-assessment**, remaining free to develop products and services with the highest degree of innovation.

5. The principle of voluntary certification helps competitiveness

Any certification involves considerable costs for companies and thus for customers. The auditing procedure itself also requires a burdensome documentation effort and is time consuming. In addition, the relevant business models and **interests of all industry sectors must be considered** for the debate regarding a certification and labelling system to be successful. Furthermore, the documentation workload and time expense of other regulatory specifications (e.g. from functional security), some of which require a significant amount of coordination, must be taken into account. Should certification be generally mandated across ICT use cases or products, it would raise barriers to entry for new market entrants, decreasing competition.

Other than for the high security area (e.g. governmental and military), companies should be **free to decide whether to take recourse to third-party certification**, depending on the customer and market requirements**. Self-declarations are also a recognised and tested means** of providing the meaningful information to the customer.

THE WAY FORWARD

We believe that public-private cooperation can play a significant role in shaping future cybersecurity strategies and practices in the EU. The Cybersecurity Private-Public-Partnership (cPPP) and AIOTI[6] are good opportunities to promote a public private dialogue based on:

- Monitoring developments and standards on cyber at a **global level** as cyber is a global issue;
- Fostering **cybersecurity training** at all levels for EU citizens, public administration and businesses;
- Encouraging **EU voluntary and industry driven cybersecurity tools**, which should be accessible, transparent, scalable across borders and focused on processes;
- Allowing **self-certification** with a declaration of security including detailed and comprehensive processes to cover;
- Evaluating national certifications to ensure that they are not given preferential treatment in procurement over international certifications;
- Promoting **security-by-design processes** to meet security profiles or goals and new **risk management models** to address cyber risks;
- Relying on **market-adopted and globally-recognised cybersecurity standards**;
- Supporting **ENISA** in mapping cybersecurity challenges and exploring effective shared solutions;
- Defining clearly goals and mechanisms to achieve **successful public-private cooperation**.

--

For more information please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Consumer and Enterprise Policy)
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

[6] The Alliance for Internet of Things Innovation was initiated by the European Commission in 2015 (http://www.aioti.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 61 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

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, 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, 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
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