Brussels, February 2018

BSA | The Software Alliance's position paper on the EU Cybersecurity Act

BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, welcomes the opportunity to provide its views on the European Commission's proposal for a Regulation on Information and Communication Technology ("ICT") Cybersecurity Certification ("Cybersecurity Act")[2]. Cybersecurity is among our members' highest priorities and is a cornerstone for the wide range of products and services they provide to customers across the EU and around the world.

We welcome the EU's Cybersecurity Act along with the continued efforts of the European Commission to strengthen the EU's cyber resilience and share the desire to continue building trust in the Digital Single Market. BSA believes that the future EU legislation must centre on outcome-focused, risk-based, technology-neutral, and adaptable certification frameworks. To ensure that the proposed EU cybersecurity certification framework set out in the Cybersecurity Act advances this objective, we encourage the co-legislators to consider the following issues when reviewing the proposed Regulation:

1. **Scope of certification schemes** – The co-legislators should seek to provide further information on what is precisely covered by the voluntary certification frameworks and clarify the scope in the Articles of the draft Regulation. The scope of the framework should focus on "processes and systems" rather than "products and services" to ensure proper alignment with existing international standards.

2. **Updates should not trigger re-certification** – Re-certification as a consequence of a software update must be approached in a proportionate manner. The Regulation should introduce a longer maximum certificate lifetime, a clear minimum certificate lifetime and a light touch renewal option.

3. **Stakeholder involvement in scheme creation request** – Stakeholders should be given the opportunity to provide meaningful input into the proposal of EU certification schemes. The European Commission should seek to create a clear "roadmap" and procedure to formalise consultation with stakeholders prior to the issuing of a request to ENISA to begin working on candidate schemes.

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With offices in Brussels, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*
BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] *COM(2017) 477*

4. **Greater emphasis on alignment with existing (international) standards** – The value of an EU certificate to entities seeking to do business both within and outside the EU hinges on equivalent, internationally-accepted standards. To avoid creating market barriers that will ultimately undermine cybersecurity in the EU, any new scheme should rely on existing international standards.

5. **Freedom of choice of conformity assessment body** – The Regulation should expressly state that manufacturers of ICT products or services may submit an application for certification to a Conformity Assessment Body ("CAB") in a different Member State to that in which the manufacturer is established.

6. **Self-certification and self-assessment –** The Regulation should explicitly call out self-certification and self-assessment as viable options. We encourage the co-legislators to introduce into the text an option for self-certification and self-assessment by the product manufacturer or service provider for products and services where agility and adaptability to the use context is important.

7. **Acceptance of EU certificates by national authorities** – The Regulation should set out in more detail how EU certificates can be used at the national level and make clear that any reference to local schemes should be read as referring to the replacement EU certification scheme.

8. **Clear and effective means of enforcement and redress** – The Regulation should set out a clear cause of action allowing certificate holders to obtain judicial redress, or powers for the national certification supervisory authority to issue decisions to rectify the failure to recognise an EU certificate.

9. **Determining whether a national certification scheme is "covered" by an EU scheme** – The Regulation should provide further clarity on how a national scheme or process will be deemed as "covered" by an EU scheme. There should be a process whereby stakeholders can seek determination from either the European Commission or ENISA as to whether a scheme "covers" the requirements of a national framework.

Issues and BSA Positions

1. Scope

a. The Regulation should clarify the scope of certification schemes

BSA welcomes the voluntary nature of the proposed schemes, which helps to preserve the ability of companies to develop and implement security solutions that protect against the latest cyber threats. However, we believe the **scope of the proposed schemes is not sufficiently clear** as the draft Regulation refers to certifying "*ICT products and services*," which are defined as "*any element or group of elements of network and information systems*" (Article 2(11)), while also referring to "*processes…systems, or a combination of those*" (Recital 47).

While such schemes under the future legislative framework are intended to be voluntary, there remains a strong potential for the schemes to become mandatory, particularly in instances where a Member State authority (national, regional, municipal) may require them for public procurement purposes. The potential for such an outcome further reinforces the need for a clear scope. Moreover, as set out in further detail below, we believe that all future schemes should seek to align with international standards, such as the ISO 27000 series. These international frameworks are primarily focused on "processes and systems" rather than "products and services." To avoid the creation of a catch-all horizontal certification approach for all cyber products, we encourage the scope to be narrowed to **focus on "processes and systems."**

Recommendation: While Recital 47 provides some clarity as to the possible scope of the future certification framework, **we encourage the co-legislators to provide further information on what precisely will be covered by the future voluntary certification frameworks and clarify the scope in the Articles of the draft Regulation.** The scope of the framework should focus on "processes and systems" rather than "products and services" to ensure proper alignment with existing international standards.

b. Updates should not automatically trigger a requirement to re-certify

For BSA members, speed of innovation is a defining characteristic of successful and secure software products and services. ICT products and services are updated frequently to improve their security, usability, performance and functionality. The draft Regulation correctly recognises the need for schemes to ensure that ICT products and services provide mechanisms for secure software updates (Article 45(g)).[3]

However, it remains unclear when a software update may trigger the need for a re-certification of the product. We stress that any **re-certification as a consequence of a software update must be approached in a proportionate manner**. Requiring entities to undergo repeated

[3] *Article 45(g) of the proposal states that the EU certification schemes must be designed to take into account several security objectives, including to ensure that ICT products and services "are provided mechanisms for secure software updates".*

conformity assessments any time a change is made – even for changes that improve security or that merely affect usability or performance – would greatly limit the appeal and success of the proposed EU certification framework. Moreover, such a requirement could create a perverse disincentive against timely updates to address identified vulnerabilities, thereby undermining rather than improving software security.

If immaterial updates were to trigger re-certification, this would compound concerns about the relatively short maximum lifetime of certificates.[4] The future framework should make clear that **updates should not automatically trigger a requirement to re-certify**. Instead, all schemes should provide a "light touch" process to assess the impact, if any, of relevant updates on the conformity of the certified ICT product or service with the certification requirements. For example, such a task could be performed, by a person designated by the manufacturer of the certified product or service (e.g. Chief Information Security Officer), who could then update the relevant conformity assessment body, or declare that during the lifetime of the certificate there have been no material adverse changes to the security of the product or service.[5]

Recommendation: We encourage the co-legislator to introduce: **(1) a longer maximum certificate lifetime; (2) a minimum lifetime, so that no scheme will be allowed to set inappropriately short renewal intervals; and (3) a light-touch renewal option** (e.g. automatic, cost-free renewal following attestation from the certificate-holder that there have been no material adverse changes to the security of the product or service).

2. Scheme Creation: Stakeholder Involvement and International Standards

a. Stakeholders involvement in relation to proposing and designing schemes

We welcome the proposed creation of a European Cybersecurity Certification Group ("the Group"), consisting of national certification supervisory authorities, to help ensure that the certification framework is implemented and applied consistently across the EU. We also welcome that ENISA will be required to closely cooperate with the Group when preparing candidate schemes, and to consult "all relevant stakeholders" (Article 44(2)).

However, given their relevant experience and insight into current and future ICT products and services and related standards, it will be **critical for industry and stakeholders from the global community to be provided the opportunity to provide meaningful input into the proposal and development of EU certification schemes.**

Recommendation: We encourage policymakers, particularly the European Commission, to **create a clear "roadmap" and procedure to formalise consultation with stakeholders prior**

[4] *Article 48(6) of the proposal would require all products and services – even those that do not receive any substantial updates – to undergo full recertification at least every three years.*

[5] *This could be similar to the task of a Data Protection Officer who, under the GDPR, must advise the company over whether a change carries such significant privacy risks that trigger a requirement to consult with the competent data protection supervisory authority.*

to issuing a request for ENISA to begin working on candidate schemes. This could be achieved by introducing (e.g., in Article 44) a means for ENISA's "Permanent Stakeholder Group" to suggest new schemes, and giving it a specific and meaningful role during each scheme's creation. This should be in addition to the possibility for industry to propose to the European Commission to consider approving an industry certification scheme as a European scheme (Recital 53).

b. Alignment with existing international standards

The European Commission correctly recognises that the growth of the cybersecurity market in Europe is restricted by overlapping standards and a lack of uniformity. As ENISA has previously pointed out, there is "*a plethora of different frameworks and standards for IT security measures.*"[6] During previous public consultations, stakeholders have consistently underlined the need for significant international alignment.

We therefore welcome that future requirements may be set out "*for example by reference to Union or international standards or technical specifications*" (Article 47(1)(b)). However, we believe that **international alignment merits greater emphasis**. BSA strongly encourages the future framework to rely on international standards, particularly the ISO 27000 series. The value of an EU certificate to an organisation that seeks to do business within and outside the EU would be undermined unless it hinges on equivalent, internationally-accepted standards. Such standards, if needed, can be transposed into European standards. The process for developing future certification frameworks at European level should not circumvent pre-existing successful international procedures. Further, we believe that any **new schemes (by referring to local standards) should not create market barriers**, either within the EU, or between the EU and third countries.

Recommendation: We encourage the proposal to be amended to state that **schemes should, *by default*, identify and align with an existing international standard,** such as the ISO 27000 series, and conform to international best practices (such as those reflected in the ISO/IEC CASCO Guidelines), when setting out detailed specifications of the cybersecurity requirements against which the specific ICT products and services are evaluated (unless such an international standard does not exist). To ensure alignment, we recommend the creation of an **obligation** whereby ENISA would be required to prepare any certification scheme in alignment with existing international standards. In those instances where ENISA seeks to deviate from existing international standards, they should be r**equired to request a "waiver"** with a clear explanation as to why international standards are not sufficient. Moreover, we strongly recommend that the **European Commission be required to consult in advance with industry**, including the cybersecurity stakeholder community, which is best placed to provide information about the standards and/or specifications that are the most relevant and effective in securing ICT products and services and preventing cyber incidents.

[6] *ENISA. "Auditing Security Measures - An Overview of schemes for auditing security measures." September 2013.*

3. EU-Wide Recognition of EU Certificates

a. Freedom of choice of conformity assessment body (“CAB”)

We welcome the clear statement in the draft Regulation that companies should be able to submit an application for certification to an accredited CAB of their choice (Recital 58). Given the Digital Single Market objectives underpinning the proposal, the Regulation should expressly state that **manufacturers of ICT products or services may submit an application for certification to a CAB in a different Member State to that in which the manufacturer is established**.

Recommendation: The Regulation should explicitly prohibit **any distinction or discrimination based on which accredited CAB issues an EU certificate, provided that the selected CAB respects the terms of its accreditation and of the EU certification scheme**.[7] No preference should be given to EU cybersecurity certificates issued by “local” CABs.

b. Self-certification and self-assessment

We believe that the draft Regulation fails to properly recognise the importance of self-certification and self-assessment. The concept of self-certification and self-assessment is widely used in certain industrial sectors and should play a role in the future EU framework. Requiring all future certification schemes to be assessed by third-party assessors across the full range of ICT products is overly burdensome. Instead, self-assessment schemes should provide organisations with access to benchmarking, allowing entities to compare their performance to similar entities. This will also help to alleviate concerns related to the disclosure of sensitive intellectual property. In such instances, rather than a close inspection of a product or service by a third-party, organisations should be allowed to seek third-party certification of the process and system surrounding the development of the product and service. This is in the line with the philosophy behind ISO 27001.

Moreover, the cybersecurity certification framework should enable flexible approaches, for instance, when a service is updated. Once a service achieves full certification then it should be possible for a service provider to complete an annual updated certification document themselves that simply states what is new in the service during that year. Self-assessment for such instances should be an option.

Standard methodologies such as predictive assurance should be encouraged to assess the security of future products or services currently under development (ISO/IEC 27034 provides guidance for predictive assurance).

Recommendation: The Regulation should explicitly call out self-certification and self-assessment as additional security compliance avenues. We encourage the co-legislators to introduce into the text **an option for self-certification and self-assessment by the product manufacturer or**

[7] *Articles 4 and 6 of the eIDAS Regulation ((EU) 910/2014) could be emulated to ensure a clear internal market principle.*

service provider for products and services where agility and adaptability to the use context is important (e.g. mass-market products or products with short lifecycles).

c. EU certificates must be acceptable under all relevant local rules and assurance processes

As set out in the draft Regulation, certificates issued as part of an EU certification scheme must be "recognised" in all Member States (Article 48(7)). While BSA welcomes this Single Market principle, we believe the proposal currently provides **insufficient detail about what "recognition" entails**. To ensure wide-spread adoption of any future framework, providers must be assured that EU certificates enable EU market access.

Recommendation: We support the views of the European Commission that schemes issuing EU certificates should, over time, replace overlapping national schemes or processes. As the proposal indicates, this will help reduce the proliferation of certification schemes. However, in order for the framework to be a success, the **proposal must set out in more detail how the EU certificates can be used at the national level**. For example, the proposal should make clear that any reference to local schemes (e.g., under local administrative or procurement rules) should be read as referring to the replacement EU certification scheme.

d. Clear and effective means of enforcement and redress

We believe that the draft Regulation lacks clarity as to what would happen if Member States, public authorities, or private bodies fail to comply with the requirement to "recognise" an EU certificate. The proposal should set out more clearly enforcement options and means of redress for certificate holders. Although European Commission action against Member States is an option, the timeframe for such action may exceed the lifetime of the certificate or the ICT product or service in question.

Recommendation: The Regulation should set out a **clear cause of action allowing certificate holders to obtain judicial redress** along with powers for the national certification supervisory authority to issue decisions to rectify the failure to recognise an EU certificate.

4. Determining Whether a National Certification Scheme is "Covered"

As previously mentioned, the Cybersecurity Act will reduce fragmentation by requiring that when an EU certification scheme comes into effect, any national scheme or "related process" that is "covered" by the EU scheme gets automatically phased out (i.e. it "ceases to have legal effect"). However, the **proposal does not clearly explain how a national scheme or process will be deemed to be "covered" by the EU scheme**. Although the proposal requires ENISA and the European Commission, when creating an EU scheme, to "*identify*" national cybersecurity schemes covering the "*same type or categories of ICT products and services*" (Article 47(1)(l)), it is unclear whether this means providing a general description (only), or listing named national schemes. If a list of “covered” national schemes is established, we believe it would be useful to introduce a process to ensure that it is kept up to date.

Recommendation: Regardless of the option chosen, we stress that there should be a process whereby stakeholders can seek determination (by ENISA or the European Commission) of whether a given scheme or process is “covered”.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315