# GSMA's Position on the EC's Proposal for the "Cybersecurity Act"

***The "Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification***

**25 January 2018**

**About the GSMA**

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.
For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

**Policy Contact:**

Dagmar Baer
Policy and Programme Advisor
dbaer[at]gsma.com

# GSMA Position on the EU Cybersecurity Act
# 25 January 2018

## Introduction

The GSMA, which represents the interests of mobile operators worldwide, welcomes the proposal of the European Commission for a review of the EU's Cyber Security strategy. The security and protection of digital services is at the forefront of mobile operators' concerns. The mobile telecommunications industry has a long history of investing in, and providing, secure products and services to their customers and strongly supports the European Commission's aim to promote trust and confidence across EU citizens and businesses using ICT services.

It is important that robust security measures are adopted by the whole digital value chain, including software and hardware manufacturers. This need is exemplified by the development of the Internet of Things (IoT) which is advancing rapidly; hundreds of thousands of new IoT services will connect billions of new IoT devices over the next decade. Security is, and will be, critical to both the success of these services, the development of this new ecosystem, and to guarantee the security and privacy of their users. Many devices and equipment which have previously not been connected to any form of network, need to have adequate security protections designed into them from the outset. The GSMA strongly supports the principles of "security-by-design" to be applied across the value chain.

It is essential that governmental institutions and public authorities support the development and adoption of aligned and cost-effective cybersecurity enablers in order to both set a good example and preserve trust and security. Practical ways in which support of these enablers could be evidenced include integrating appropriate security requirements and liability clauses for suppliers into public procurement practices.

Education and awareness of consumers of ICT products and services, enabling them to make informed purchasing decisions is a prerequisite for "Cyber-secure" markets. Efforts are required beyond industry engagement, including improving citizens' awareness and developing their digital skills from a young age. Coordinated action at EU level promoting investment in professional and educational training programs in schools, colleges, universities and research centres will help the development of a skilled work force and cyber-responsible citizens.

## On the EU Cyber Security Certification Framework

<u>General context on certification schemes</u>

The GSMA welcomes the EU's focus on enhancing cybersecurity across Member States. It is important to industry, however, that the proposed certification framework minimizes duplication and fragmentation across Member States, reduces compliance costs and promotes a more secure European and global ICT market.

In that sense, GSMA members consider that the establishment of an EU certification framework should build upon existing national and international certification standards, especially those defined by industry, such as those promoted within the GSMA IoT Security Guidelines, while taking into

account the global dimension of the ICT market for products and services. Utilizing existing standards would help leverage existing experience and technical knowledge of people and organisations in this specialized and complex field whilst ensuring that the EU scheme has a minimal (financial or otherwise) impact.

Governance and stakeholder's involvement, art 44 & art 55

The Act has a very wide scope, potentially covering all ICT products and services. GSMA recommends the scope, governance and supporting processes defined within the Act should be further clarified in order to define more precisely the decision-making processes and ensure that stakeholders from all sectors and Member States, including EU private entities, are meaningfully involved and engaged in the process. For instance:

- It is not fully clear who the owner of any given certification scheme is: does the European Commission (EC) request ENISA to prepare a scheme, or, does the new European Cybersecurity Certification Group (ECCG) perform this role.
- It is unclear whether the EC has to adopt any scheme defined or recommended by ENISA or whether it has room for maneuver to adapt or disregard such recommendations;
- For the ICT products and services that will be covered by the scope of article 49 (see below), it is unclear why Member States would only have an advisory role in this process. It would seem more justified, especially given the reality of expertise in the area at this point of time, to follow the examination procedure in Art. 5 of Regulation no182/20 11, thereby giving Member States a more decisive role in determining the adoption of an implementing act and not simply an advisory role.
- The Act should also be improved to clarify the roles of each entity, both at national and European levels, in the monitoring and implementation of the certification schemes defined at EU level; this would ensure, once a given certification scheme is applied, a more harmonised implementation is achieved across the EU.

Finally, EU industry from all sectors and Member States should be more actively involved, and not only consulted, in the discussions between the Commission, ENISA and the ECCG.

Assurance Level, art 46

The GSMA recommends that the need for all certification schemes within the framework to provide "Basic", "Substantial" and "High" assurance levels to be defined on a case-by-case basis within the certification schemes themselves. It is indeed easy to envisage the creation of certification schemes that only require one level of assurance and other schemes that require multiple levels. The "Basic" assurance level should provide a solid basis to guarantee the security and privacy of its user(s).

When defining a level of assurance, each scheme must utilize existing security standards in a way that harmonizes the new scheme with current approaches across Member States.

We recommend the Act has a solution for how "state of the art" security threats are addressed by the certification schemes to ensure the schemes' address new cyber security issues in what is an ever-changing threat landscape. We recommend that each scheme is required to address this issue

when defining its assurance level by, for example, use of industry common practices such as continuous risk assessments, ethical hacking/pen-testing, bug bounties, coordinated vulnerability disclosure schemes etc.

Voluntary scheme, art 48 (2)

The Commission is proposing a voluntary approach to cyber security certification schemes. The GSMA considers this measured approach appropriate at this stage because the scope of the Act is wide and certain key ICT markets (in particular the IoT market) are at a nascent stage in Europe and globally. A compulsory certification scheme applicable across the board for all ICT products and services could represent a cost that some small manufacturers cannot bear, could significantly delay the rollout of services, may stifle innovation and may not have the intended security impact.

After this initial stage, and depending on the maturity of implementation in EU Member States and the criticality of a product or service, we recognize that, in the future, potentially mandatory schemes for certain ICT products and services may begin to evolve in a phased approach. Should that happen any mandatory scheme should be accredited by national accreditation bodies by default- thus reinforcing the grounds for trust.

EU certification scheme validity period, art 48 (6)

The draft Act defines a validity period of three years for any EU certification scheme. It does not seem appropriate to fix such a value in the Regulation and for all types of EU certificates. The Act should allow the duration of each certificate to be defined on a case by case basis.

Relationships between EU certification schemes and national schemes, art 49

The draft Act states that once a certification scheme is adopted at EU level, any national scheme relating to the same ICT products and services shall cease to exist.

While EU harmonisation will be certainly welcome on many aspects, especially for IoT products and services, some areas still have to be governed by national rules; the Act should thus clarify that it does not cover the following sensitive areas:

- National Security;
- Sectors of vital importance to Member States, such as telecoms, health or electricity infrastructures;
- National Defense.

These areas should be under the sole responsibility of Member States and their concerned national security agencies unless they would decide differently in future.

Finally, the relationships between the proposed EU scheme and the pre-existing and implemented international security standards and certification schemes are unclear. Such pre-existing industry standards and certification schemes will remain relevant in their international use and application, beyond the scope of the Union, even when the EU issues a certification scheme of its own making.

**ENISA mandate**

The GSMA supports the re-evaluation of ENISA's role. In the proposed "Cybersecurity Act", ENISA's mandate is pre-eminently supportive in nature, which is welcome.

For ENISA to build the skills, capabilities and capacity to support Member States and industry in an effective and competent manner would, require a substantial effort in terms of both time, financial resources and the ability to attract the right talent. We therefore recommend that ENISA should work together with the experts of that field, and impacted parties, when creating a new scheme as this reduces the burden of knowledge needed at ENISA. In particular, ENISA should collaborate with security experts from national security agencies who already have a sound experience of certification matters gathered over 15 years of certifications within SOGIS-MRA.

Finally, ENISA should ensure that a representative group of EU industry is effectively involved in its work and decision-making processes.