European Automotive and Telecom Alliance

Third High-Level Meeting on Connected and Automated Driving

Gothenburg, 18 June 2018

Regulatory briefing paper

Topic: Cybersecurity

Context: Cybersecurity Act

Short description: Renewing ENISA's mandate and Creation of an EU Framework for Cybersecurity Certification of ICT products & services

Status: The Cybersecurity Act: issued by the European Commission in September 2017. Currently under review in Council and EP.

EATA's position on the EC's proposal for the "Cybersecurity Act"

EATA welcomes the proposal of the European Commission (EC) for a review of the EU's Cybersecurity strategy. The security and protection of digital products and services, in an increasingly connected society, are at the forefront of our concerns. Telcos, Vehicle Manufacturers and Automotive suppliers have a long history of investing in, and providing, secure products and services to their customers and, strongly support the EC's aim to promote trust and confidence across EU citizens and businesses using our products and services.

It is important that robust security measures are adopted by the whole digital value chain, including software and hardware manufacturers. Security will be critical to the success of our respective products and services as we need to guarantee the security and privacy of their users. Many devices and equipment, or vehicles, which have previously not been connected to any form of network, need to have adequate security protections designed into them from the outset. EATA strongly supports the principles of "security–by-design" to be applied across the value chain.

Education and awareness of consumers of products & services is critical also in ensuring that they can make informed decisions about the purchasing of 'cyber secure' product/services.

On the EU's Cybersecurity Certification Framework

EATA welcomes the EU's focus on enhancing cybersecurity across Member States. It is important to industry, however, that the proposed cybersecurity framework minimises duplication and fragmentation across Member States, reduces compliance costs and promotes more secure European and global ICT & automotive markets.

EATA considers that the establishment of an EU certification framework should build upon existing national and international certification standards and regulations such as the regulations on automotive cybersecurity and on over the air software updates, currently being drafted at the UN-ECE WP 29. Utilising existing standards would help leverage existing experience and technical knowledge of people and organisations in this specialised 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. EATA recommends the governance and supporting processes defined within the Act be further clarified in order to define more precisely the decision-making processes and ensure that stakeholders from all sectors, especially EU private entities, and Member States, are meaningfully involved and engaged in the process. Notably, EU industry should be able to propose and be actively involved in the definition of schemes relevant to their industry. Member States should also be given that competency as well as a stronger role in the comitology process before EC adoption of a given scheme

Assurance levels (Art. 46) & Validity period of schemes (Art. 48(6))

EATA recommends that the need for all certification schemes within the framework to provide "basic", "substantial" and "high" assurance levels should be defined on a case-by-case basis within the certification schemes themselves. The validity period of a scheme should also be defined on a case by case basis. The draft Regulation should therefore be amended and simplified in those regards. No one size fits all!

Voluntary schemes (Art. 48(2))

EATA considers the Commission's proposal to grant EU Cybersecurity schemes a voluntary natureas essential. It is appropriate at this stage because the scope of the Act is wide and certain key ICT markets are at a nascent stage in Europe and worldwide. A compulsory certification scheme applicable across the board for all ICT products and services would 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 by EU Member States, and also the criticality of the product or service, we recognise that, in the future, potentially mandatory schemes for certain ICT products and services may begin to evolve in a phased approach.

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. It should be noted however, that whilst EU harmonisation is most certainly welcome, some specific sensitive areas still have to be governed by national rules (national security, sectors of vital importance to Member States, national defence) and under the sole remit of the Member States.

On the renewed mandate of ENISA

EATA supports the re-evaluation of ENISA's role. This role and mandate is pre-eminently supportive in nature, which is welcome.

ENISA should work together with the relevant experts and impacted parties when laying down the groundwork for the new schemes. 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 for example. ENISA should ensure industry involvement at all levels of the decision-making process, and especially representatives of the EU industry concerned by a given scheme.