EUROSMART
The Voice of the Digital Security Industry

Cybersecurity Act:

Five outcome-based principles from the digital security industry

The proposal for a Cybersecurity Act is a matter of European industrial policy and economic growth as well as being of importance for European digital sovereignty and societal choices.

The level of resistance to potential attacks on European encryption solutions will be key to the technical transposition of articles 7 and 8 of the European Union Charter of Fundamental Rights.

The Cybersecurity Act is part of the new social contract for the digital age. Therefore, we will bear the responsibility for drawing up fair provisions which uphold the interests of European citizens, Member States, European industry, the European Institutions and the digital single market. We must make sure that the process of establishing confidence in products through a new ENISA-led certification framework is beneficial, first and foremost, to European citizens.

With this vision in mind, Eurosmart invites both co-legislators to take 5 critical points into account when considering the initial proposal from the European Commission.

- Firstly, **clear legal definitions of essential terms** referring to IT and security ecosystems (aka “cybersecurity”).

- Secondly, **fair and open European governance** during the preparation phase of candidate European certification schemes.

- Thirdly, **a well-defined European certification objective** that is apt for each level of certification. Above all, the co-legislators should ensure that the ‘substantial’ and ‘high’ levels require mandatory penetration testing (“pentest” or “ethical hacking”) of the product by Conformity Assessment bodies (CABs) whilst a product is being evaluated.

- Fourthly, **European standards must be the basis** for the preparation of a new candidate European certification scheme.

- And finally **ENISA’s “Intellectual Property Rights” (IPR policy)** should be spelled out in the Cybersecurity act.

Appendix:

Development of the five outcome-based principles from the digital security industry

1. Clear legal definitions of essential terminologies

This regulation is about to define a new framework that enables the creations of certification schemes to be mutually recognised by all the Member States. With the aim at ensuring a legal certainty the following terms shall be clearly defined:

- Asset
- Attack method
- Attack potential
- Breach of data
- Certification
- Conformity
- Composite Certification
- Ethical Hacking
- European Cybersecurity
- Evaluation
- Evaluation method
- Hackers
- Internet
- IT & Security
- Pentest ("Penetration testing" or "industrial ethical hacking")
- Product
- Resilience
- Robustness
- Services
- Sub-product
- Target evaluation
- Vulnerability
- Vulnerability Automatic testing tool
- Vulnerability Manual testing tool

2. Fair and Open European Governance

- Due to the sensitive nature of IT and security products and services, which are key elements of European digital sovereignty, Regulation (EC) No 765/2008, which sets out the requirements for accreditation and market surveillance relating to the marketing of products, cannot be deemed applicable. This regulation refers to the European Accreditation Arrangement which currently covers 36 full member states and 14 associate member states.

- Implementing acts shall establish a dedicated mutual arrangement for IT and security Conformity assessment bodies (CABs).

- Mandatory validation of any new certification scheme by the ENISA Permanent Stakeholder Group (PSG), which brings together cybersecurity experts recognised as such by the cybersecurity ecosystem and academics.

- Due to the sensitive nature and the economical and societal impacts of a new certification scheme, ENISA must be able to draw on the services of experts to prepare a new certification scheme without having recourse to external consultants. We should also keep in mind that whilst the certification scheme will initially operate on a voluntary basis, it will become mandatory in sectorial EU law if cyberattacks cause serious damage to EU citizens, institutions, industry, and member states.

- The European Cybersecurity Certification Group (the 'Group'), consisting of national certification supervisory authorities of all Member States (as defined in article 44 of the regulation), should efficiently implement checks and should set-up for each certification scheme a group of permanent experts in charge of accrediting and performing a technical audit of the CABs of all Member States. Such a permanent group will de-facto ensure the homogeneity of certification across member states from the outset of the scheme.

- The Group or an industry representatives body shall have the ability to propose the preparation of a new certification scheme in order to favour the harmonisation of certification practices across business segments and the Member States.

- When preparing candidate schemes, ENISA shall conduct a public consultation with a minimum period of 3 months for submissions to be presented to ensure that all relevant stakeholders and the Group are consulted in addition to the Group.

3. Well-defined European certification objectives

- A European certification system should be feature a range of levels of certification. Above all, the co-legislators should ensure that the 'substantial' and 'high' levels require mandatory pentesting ("industrial ethical hacking") of the product by Conformity Assessment bodies (CABs).

Levels	What is tested	Assessment type
High	Compliance & Robustness	CABs performing penetration tests by ethical hacking
Substantial	Compliance & Robustness	
Basic	Compliance	CABs performing conformity tests
		No CABs: Self-certification

- Each certification scheme should clearly define the following:
  - Target of evaluation;
  - Asset to be protected;
  - Attack potential;
  - Robustness level.

4. European Standards must serve as the basis for the preparation of a new candidate European certification scheme

When preparing a new candidate European certification scheme, ENISA should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and resilience of European certification schemes.

European certification schemes shall only assess the security requirements and not a product's functional requirements. This approach seeks to encourage permanent and continuous innovation in all European industry sectors while increasing the level of robustness of European products and services.

Typical product or service pillars:

Functional specification	Conformity against functional specification	Privacy certification	Security certification
CEN /CENELEC/ETSI/ITU or proprietary	Assess conformity with the functional standard	GDPR/ePrivacy Ongoing definitions of Privacy certification schemes	Cybersecurity Act: certification schemes
Currently in used by all European industrial sectors		Ongoing / under definition	Today only SOG-IS or private schemes such as EMVCo are existing

5. ENISA's "Intellectual Property Rights" (IPR policy)

ENISA will be producing certification schemes which should be considered as technical documents that may refer to technical reports prepared by industry fora and consortia and could therefore contain essential patents.

Standards rely on technical contributions from various sources. These contributions may contain patented technologies and other protected rights, commonly known as Intellectual Property Rights. When it is not possible on technical grounds to produce or use equipment or methods which comply with a standard without infringing IPRs, i.e. without using technologies that are covered by one or more IPR, the IPR policy in question is referred to as 'essential'.

A well-defined IPR policy is an essential element of the chapter III of the Cybersecurity act.

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, security evaluation laboratories, High Security Hardware, Biometric technology providers, terminals, system integrators, application developers and issuers who work in dedicated working groups (security, electronic identity, communication, Cybersecurity, marketing). Members are largely involved in research and development projects at European and international levels.

Eurosmart members are companies (Fingerprint Cards, Gemalto, Giesecke & Devrient, GS TAG, Idema, Imprimerie Nationale, Infineon Technologies, Inside Secure, Linxens, Nedcard, NXP Semiconductors, +ID, Real Casa de la Moneda, Samsung, Sanoïa, STMicroelectronics, Toshiba, Trusted Objects, WISekey, Winbond), laboratories (CEA-LETI, Keolabs), research organisations (Fraunhofer AISEC), associations (SCS Innovation cluster, Smart Payment Association, Mobismart, Danish Biometrics).

Contact:

Pierre-Jean VERRANDO
Director of operations
pierrejean.verrando@eurosmart.com
Mobile: +32 471 34 59 64

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue du Luxembourg 19-21 | B-1000 Brussels | Belgium
Tel: +32 2 506 88 38 | Fax: +32 2 506 88 25