EUROSMART
The Voice of the Digital Security Industry

Revision of the Cybersecurity Act (CSA)

The importance of maintaining efficient governance

Eurosmart representing the Digital Security Industry welcomes the initiative to extend the scope of the European Cybersecurity Certification Framework as outlined in the Cybersecurity Act (CSA). With over 25 years of active involvement, the digital security industry has been a pioneer in Cybersecurity certification in Europe, providing essential insights for Common Criteria in Europe[1] and shaping the forthcoming 'EUCC', the first European cybersecurity certification scheme.

Managed security services play a crucial role in preventing, detecting, responding to, and recovering from cybersecurity incidents. Including such types of services in the European certification framework is the right approach for enhancing the capabilities of the European cybersecurity value chain.

The CSA establishes an efficient governance structure within the European Cybersecurity Certification framework to support the preparation, the adoption, and the maintenance of the schemes. This approach deserves the engagement and active collaboration of industrial actors, conformity assessment bodies, and private stakeholders, in conjunction with public authorities, to ensure that each scheme attains the requisite level of trust. The existing CSA approach strikes a balance between security, trust and efficiency, recognising the importance of time-to-market consideration in scheme development and maintenance. A flexible approach is a prerequisite for a swift market adoption.

Extra control layer for scheme development and maintenance to compromise efficiency

From this standpoint, Amendment 40 from the ITRE Committee of the European Parliament, introduces complexity. The example of the European Cybersecurity Cloud Scheme (EUCS) mentioned in support of Amendment 40, remains a specific case that surpasses the initial objectives of the revision of the Cybersecurity Act. Eurosmart believes that other tools could be enabled to address the political issues specific to the EUCS.

Through its proposal the European Parliament, modifies the delegated powers of the Commission regarding the "*Preparation, adoption, and review of a European cybersecurity certification scheme.*" (art. 49) thought implementing acts. This approach empowers the European Parliament to exercise veto power over the Commission's proposals. However, since the objectives of these delegated powers should only focus on technical matters, this additional control brings more complexity and slows downs the approval process.

[1] Eurosmart hosts two of the technical groups of the SOGIS (Senior Officials Group Information Systems Security): the JIL Hardware-related Attacks Subgroup (JHAS) and the International Security Certification Initiative (ISCI WG-1). See more: https://www.sogis.eu/documents/mra/201802-SOGIS-Position.pdf

To maintain efficiency and meet market expectations in security, the adoption and regular update of technical documents need to be flexible and promptly executed. The European Parliament's involvement in highly technical matters could impede the process without adding technical value. In a comparative context, the European Parliament does not endorse harmonized standards in conformity and safety-cybersecurity-related areas: the Commission delegating their development to the European Standardisation Organisations (ESOs).

Existing safeguards for schemes developments and maintenance

The European Cybersecurity Certification Framework already incorporates safeguards and counterpowers through the European Cybersecurity Certification Group (ECCG), which comprises Member States' experts and representatives and potential sub-groups to oversee the evolution of different schemes.

Eurosmart fears that such an overregulation may undermine the efficiency of the entire EU cybersecurity scheme framework and invites the legislator to consider the side-effects on the other future schemes.

To anticipate any political and technical issues when drafting, amending, and updating European certification schemes, Eurosmart calls on a better coordination between the ECCG and relevant public and private stakeholders. The latter could be achieved through the creation of recognized partnerships with the European cybersecurity certification ecosystem.

Enhancing a trusted ecosystem to support schemes' adoption and maintenance

Eurosmart recognises room for improvement in the current governance practices. However, introducing an additional layer of control is not a viable solution. A trusted ecosystem of experts representing diverse stakeholders already exists. This active community is part of the legacy of the technical groups of the SOGIS (Senior Officials Group Information Systems Security), which has been delivering updated document for the creation of the EUCC scheme. Moreover, additional pools of contributors around new certification technical domains (Cloud, 5G..)[2] have already been established around ENISA.

From this starting point, Eurosmart considers that further efforts should be directed toward enlarging and organising this community through specific partnerships. Eurosmart has consistently advocated for the development of an ISAC[3] model to accommodate this expanding community. ISAC remains the preferred solution within the digital security ecosystem to facilitate organised contributions and foster a continuous dialogue with public authorities.

[2] ENISA has established 3 ad-hoc working groups public agencies and private stakeholders for the setting-up of the future EU cybersecurity certification schemes (5G cybersecurity certification, Cloud Services, transposition of SOG-IS MRA) https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls

[3] Information Sharing and Analysis Centers (ISACs) are non-profit organizations that allow two-way sharing of information between the private and the public sector. This model is fully applicable to schemes' maintenance https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European 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.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com

@Eurosmart_EU

@Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com