



Cybersecurity Act 2 (CSA2) Proposal

ENISA's mandate in short

Area	CSA	CSA2 proposal
EU policy support	Guidelines, reports, through NIS Cooperation Group Capacity-building Research and innovation tasks International cooperation	Clear emphasis on support in implementing cybersecurity laws and policies Tailored support to specific sectors (i.e. health) Capacity-building International cooperation in line with EU policies/priorities
Standards and certification	ENISA monitoring standards for schemes only	ENISA drafting technical specifications to support Union legislation, e.g., CRA and certification ENISA actively contributing CRA standardisation and international standards
Operational cooperation	ENISA secretariat of EU-CyCLONE and CSIRTs network	ENISA member of CSIRTs network Situational awareness (sharing early warnings, analysis, use of secure communications tool) Stronger role in vulnerability management (e.g., enriching vulnerability services, providing advisories) Managing platforms for incident and vulnerability reporting Support for incident response
Skills	No concrete tasks – objective only	Implementation of Cybersecurity Skills Academy Develop European cybersecurity skills attestation schemes and authorise providers to deliver attestations
Ransomware	-	Helpdesk to help entities respond to and recover from ransomware attacks, in cooperation with Europol Monitor trends in techniques, demands and impact of ransomware attacks

European Cybersecurity Certification Framework

Area	CSA	CSA2 proposal
Scope	ICT products, ICT services, ICT processes or managed security services; Unclear whether non-technical risk factors excluded	CSA1 + cyber posture of entities (NIS2 and beyond); Non-technical risk factors excluded – to be dealt with in Trusted ICT Supply Chain framework
Smooth Procedure	Lack of clarity on roles, no predictability and delays maintenance not covered	Clarified procedures for requesting & developing schemes, legal timelines (1 year as a rule for development of a candidate scheme) ENISA role as “scheme manager” on maintenance
Simplification tool	Misalignment with NIS2; ad-hoc alignment with CRA	Facilitate compliance with CRA & NIS2 and potentially other legal acts
More inclusive stakeholder engagement	Stakeholder Cybersecurity certification group (SCCG), Union Rolling Work Programme (URWP)	Flexible planning through a dedicated Commission website providing up-to-date information Reporting obligation to the co-legislators European cybersecurity certification Assembly
Financing	EU Budget	Partly fee-based

ICT supply chain security

What?

- The security of the Union.

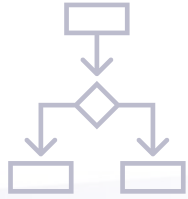
Why?

- The threats and risks affecting the cybersecurity of our critical infrastructure are dramatically increasing.

How

- With a horizontal, technological-neutral framework to protect Member States and the Union by addressing strategic ICT supply chain risks and monitor dependencies in an evolving cyber threat landscape.
- Targeted and proportional nature (limited share of companies in NIS2 scope + only critical ICT assets)
- Simple for companies to implement – specific restricted entities are listed
- Market impact never neglected (assessment of economic and societal impacts)

ICT supply chain security



Proportional and targeted - Initiated by COM or at least 3 Member States or emergency procedure initiated by COM:

risk assessments, identification of key assets and risk based, proportionate mitigating measures based on market analysis and thorough assessment of economic and societal impacts, including restriction on suppliers from countries posing cybersecurity concern

Possibility to restrict specific third country companies under exceptional circumstances



Outcome (implementing involving Member States):

Identification of countries posing cybersecurity concerns (criteria)

Identification of key ICT assets, mitigation measures (incl. poss. restrictions) and transition period for specific supply chains in specific critical entities

Identification of entities established in a designated country posing cybersecurity concerns, or controlled by such third country, by an entity established in such third country, or by a national of such third country



Possible exemption for entities from designated countries:

COM decision based on assessment upon an application from the entity

Register for exempted entities

State-of-play

Thank you

