



**The Parliament of Romania  
Senate**

Bucharest, 18<sup>th</sup> December 2017

Courtesy translation

**OPINION of the ROMANIAN SENATE**

**to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the „EU Agency for Cyber Security”, repealing Regulation (EU) 526/2013 and on Cyber Security Certification for Information and Communication Technologies („Cyber Security Act”)  
- COM (2017) 477 final -**

The Romanian Senate, pursuant to art. 67, art. 148 (2) and (3) of the Romanian Constitution and the Protocol no.2 annexed to the Treaty of Lisbon amending the Treaty on European Union and the Treaty on the Functioning of the European Union, signed in Lisbon in 13<sup>rd</sup> December 2007, has examined the **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the „EU Agency for Cyber Security”, repealing Regulation (EU) 526/2013 and on Cyber Security Certification for Information and Communication Technologies („Cyber Security Act”) - COM (2017) 477 final.**

Having in view the report of the Committee for European Affairs from 7<sup>th</sup> December 2017, **the Romanian Senate**, issued on 18<sup>th</sup> December 2017 an OPINION, as follows:

(1) **establishes** that **the legal basis** of the proposal for a Regulation is based on the provisions of Article 114 of the Treaty on the Functioning of the European Union (TFEU), which refers to the approximation of the laws of the Member States in order to achieve the objectives set out in Article 26 of TFEU, namely the proper functioning of the internal market.

(2) **notes that the choice of legal form is *the regulation***, since ENISA has been set up by means of a regulation, the same legal instrument considered appropriate also for this proposal. Also, due to the important role played by the Agency in creating and managing an EU framework for cyber security certification, the new mandate for the agency and the above-mentioned framework are best set in a single legal instrument, the regulation.

(3) **notes that this proposal for a regulation respects the principle of subsidiarity** because, in the current context of threats and cyber-security risks, it results that, in order to increase the Union's collective cybernetic resilience, the individual actions of the EU member

states and the fragmented approach to cyber security will not be enough. Cyber security has become a matter of common interest for the EU.

**(4) notes that this proposal partly respects the principle of proportionality.**

Cyber security is a security dimension as a whole, and the competence and expertise on security assessment belong to the member states. Indeed, the management of the area of freedom, security and justice is a shared competence between the Union and the member states (Article 4 TFEU), but given the impact of cyber security on national security, it is in many respects a matter of national sovereignty.

For this reason, as regards the single European certification framework, it argues that **the role of the member states** and, implicitly, of the national certification authorities, **should not be reduced to an advisory one**. Member States should have a consistent role in the new architecture of cyber security certification, given their expertise.

**(5) considers necessary and appropriate to review** the status and mandate of ENISA and welcomes granting of a permanent mandate for this agency, which, in the context of the implementation of the NIS Directive, has a much more important role to play.

**(6) supports** this proposal for a regulation, believing that this initiative will help to increase users' confidence in the digital market through: the interest expressed in ensuring the cyber security, the setting of strategic objectives and concrete actions aimed at achieving resilience, reducing cybercrime, the development of cyber defense policy and capabilities, the development of industrial and technological resources.

**(7) draws attention** to the possibility of developing the operational capacity of the Agency, as the exchange of information among states concerning the cyber incidents at the European level is predominantly voluntary.

**(8) considers that clarification is needed** regarding the regulatory text concerning the European Cyber Certification Framework. An example in this respect is the argument set out in paragraph 56 of the preamble to the proposal:

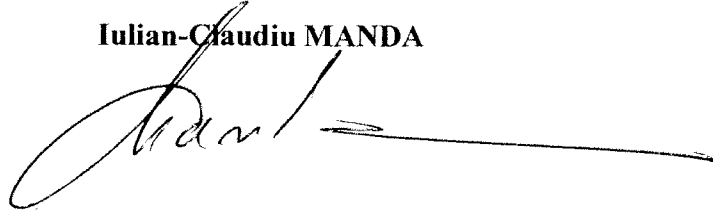
„The Commission should be empowered to address ENISA the request to prepare proposals for systems for specific ICT products or services. On the basis of the ENISA system proposal, *the Commission should be empowered afterwards to adopt the European Cyber Security Certification System by means of implementing acts*”.

Although certification at European level can benefit from increasing consumer confidence in ICT products and services, **this can be a very costly process** for manufacturers and suppliers, which in some cases, **can lead to higher prices for consumers**, and it is necessary to clearly specify who and how it will regulate the certification process.

**(9) calls** for an in-depth analysis at the level of the Cyber Security Operational Council, established through the National Cyber Security Strategy of Romania, in close connection with the market players, regarding the new measures concerning the certification in the field of cyber security.

**p.President of the Senate**

**Iulian-Claudiu MANDA**

A handwritten signature in black ink, appearing to read 'Iulian-Claudiu MANDA', with a long horizontal flourish extending to the right.