EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)

2017/0225(COD) - 13/09/2017 - Legislative proposal

PURPOSE: to enhance the organisational aspects of ENISA, the EU Cybersecurity Agency, with a view to ensuring an adequate level of cybersecurity in the Union and repeal Regulation (EU) 526/2013 on Information and Communication Technology cybersecurity certification (Cybersecurity Act).

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: the European Union has taken a number of actions to increase resilience and enhance its cybersecurity preparedness. Since the first EU Cybersecurity Strategy adopted in 2013, important developments have taken place, including the second mandate for the European Union Agency for Network and Information Security (ENISA) and the adoption of the Directive on security of network and information systems (NIS Directive), which form the basis for the present proposal.

In 2016 the European Commission adopted a Communication on Strengthening Europe's Cyber Resilience System, in which further measures were announced to increase the EU’s resilience and preparedness.

The Council recalled that the ENISA Regulation is one of the **core elements of an EU cyber resilience framework** and called upon the Commission to take further steps to address **issue of certification** at the European level. In 2017, it welcomed the Commission's intention to review the Cybersecurity Strategy in September and to propose further targeted actions before the end of 2017.

IMPACT ASSESSMENT: the impact assessment sought to mitigate problems such as the fragmentation of policies and approaches to cybersecurity across Member States; dispersed resources and fragmentation of approaches to cybersecurity across EU institutions, agencies and bodies; insufficient awareness and information of citizens and companies, coupled with the growing emergence of multiple national and sectoral certification schemes.

The analysis led to the conclusion that a **reformed ENISA** in combination with an EU general **ICT cybersecurity certification framework** was the preferred option.

CONTENT: overall, the proposal **reviews the current mandate** of ENISA and lays down a **renewed set of tasks and functions**, with a view to effectively and efficiently supporting Member States, EU institutions and other stakeholders' efforts to ensure a secure cyberspace in the European Union.

The new proposed mandate seeks to give the Agency a **stronger and more central role**, in particular by also supporting Member States in implementing the NIS Directive and to counter particular threats more actively (operational capacity) and by becoming a centre of expertise supporting Member States and the Commission on cybersecurity certification.

Specially, it proposal seeks to establish:

-

- an **EU Cybersecurity Agency**, building on the European Agency for Network and Information Security (ENISA), which will improve coordination and cooperation across Member States and EU institutions, agencies and bodies;
- an **EU cybersecurity certification framework** that will ensure the trustworthiness of the billions of devices ("Internet of Things") which drive today's critical infrastructures, such as energy and transport networks, and also new consumer devices, such as connected cars.

An EU Cybersecurity Agency: the Agency will be given a **permanent mandate** to assist Member States in effectively preventing and responding to cyber-attacks. It will improve the EU's preparedness to react by organising yearly pan-European cybersecurity exercises and by ensuring **better sharing of threat intelligence and knowledge** through the setting up of **Information Sharing and Analyses Centres**. It will help implement the Directive on the Security of Network and Information Systems which contains reporting obligations to national authorities in case of serious incidents.

The Cybersecurity Agency would also help put in **place and implement the EU-wide certification framework** that the Commission is proposing to ensure that products and services are cyber secure. The proposal also includes the provisions facilitating the combating of **fraud**, corruption and other unlawful activities as well as **staffing and budget** provisions.

An EU cybersecurity certification framework: at present, a number of different security certification schemes for ICT products exist in the EU. The Cybersecurity Agency, ENISA, will put in place and implement this certification process. The proposed EU-wide certification framework creates a comprehensive set of rules, technical requirements, standards and procedures to agree each scheme. Each scheme will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards.

The proposal establishes the main legal effects of European cybersecurity certification schemes, namely (i) the obligation to implement the scheme at national level and the **voluntary** nature of certification; (ii) the invalidating effect of European cybersecurity certification schemes on national schemes for the same products or services. It also lays down the procedure for the adoption of European cybersecurity certification schemes and the respective roles of the Commission, ENISA and the **European Cybersecurity Certification Group**.

BUDGETARY IMPLICATIONS: the total appropriations for ENISA, including administrative expenditure, from 2019 to 2022 is estimated at **EUR 86.038 million**.