RÉPUBLIQUE FRANÇAISE

COMMISSION
DES
AFFAIRES EUROPÉENNES

Paris, le 16 novembre 2017

Draft resolution on

the proposal for a regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

adopted by the European affairs committee on November 9, 2017

EUROPEAN RESOLUTION MOTION
BEARING REASONED OPINION

① The Regulation proposal COM (2017) 477 final on cybersecurity aims to reinforce the European Union Agency for Networks and Information Security (ENISA) and to set up a European cybersecurity certification framework on products and services of information and communication technologies.

② It sets six targets:

③ – to develop the means and the preparation of Member States;

④ – to improve cooperation and coordination across Member States and European Institutions;

⑤ – to increase the means on an EU wide level in order to complement the actions of Member States in case of cross-border cyber crisis;

⑥ – to raise the awareness of individuals and companies on cybersecurity issues;

⑦ – to enhance the overall cybersecurity transparency and insurance;

⑧ – to avoid the multiplication of certification schemes within the Union, as well as security requirements and evaluation criteria in the different Member States.

⑨ In order to achieve those objectives, the Commission proposes to reinforce the ENISA to become a major player on European cybersecurity, when it is currently only an Agency with limited means and whose term will come to an end in 2020.

⑩ The ENISA would receive a permanent mandate. Its fields of action would be extended to new missions regarding the market, the cybersecurity certification and the standardization as well as technical assistance in the case of significant incidents. It would maintain its missions regarding, firstly, the conception and

implementation of the European policy on cybersecurity matters, but also the support for capacity building (means and skills) for Member States, operational cooperation and crisis management.

⑪ The ENISA would thus be sustained and see the full extension of its capabilities. It could then conduct technical investigations within the Member States, following a notification of a cybersecurity incident at a European scale, on Member States or Commission's request. It could also provide a technical assistance to some Member States in the case of a cyber attack, by means of a response team.

⑫ The proposal provides in a second part the establishment of a unique certification framework reflecting the products' and services' level of security of information and communication technologies in the European Union, of which the ENISA would become the referral authority. A single window would allow the products certification for companies.

⑬ While today the competence and expertise regarding security assessment belong to Member States, the proposal grants this competence to the ENISA. Furthermore, once the European scheme is created, any national certificate would be deleted and it would no longer be possible to adopt another one, even if it proposes a higher security level. For all products and services, the draft scheme provides three insurance levels: elementary, substantial and high.

⑭ Having regard to article 88-6 of the Constitution,

⑮ The French Senate makes the following observations:

⑯ – the Senate supports European capacity building regarding cybersecurity matters and the necessity to have a unique European cybersecurity certification framework for products and services on information and communication technologies, as well as for cybersecurity systems;

⑰ – however, it considers that these two subjects should constitute two different texts, one setting the ENISA's mandate, and the other one establishing a framework for certification;

⑱ **Regarding Member States' competence on security matters:**

⑲ – the Senate underlines that cybersecurity, given its importance for Member States' security, is on several aspects an area of national sovereignty;

⑳ – consequently, Member States must keep, on the one hand, their faculty to adopt norms and standards providing a higher security level and on the other hand, their full place on the new European device, based on their voluntary participation to a European cybersecurity;

㉑ – for that reason, as regards to the proposal's legal base, it considers that a Regulation on cybersecurity cannot only deal with the functioning of the internal market (articles 26 and 114 of the Treaty on the Functioning of the European Union), but it also has to integrate security issues (article 5 of the Treaty on European Union);

㉒ **Regarding the ENISA's revised mandate:**

㉓ – the Senate considers that all Member States must dispose of enough technical and operational capacities on cybersecurity matters. It would be welcome that the ENISA supports and backs them in this process. This implicates that the ENISA does not replace the operational capacities of Member States and do not have a reaction team in case of crisis, which creation is unjustified;

㉔ – the Senate recalls that the European cooperation on cybersecurity matters must continue to be done on the basis of the Member States' participation and voluntary provision of sensitive information, even those related to national security on which the ENISA cannot therefore dispose of further investigatory powers as planned in the article 7, point 5 of the Regulation proposal;

㉕ **Regarding the cybersecurity certification:**

㉖ – the Senate points out that the Regulation proposal places the ENISA at the heart of the certification process, while this agency has no expertise on the matter;

㉗ – it recalls that the actions that have been taken for many years by a majority of Member States, including France, helped turning

Europe into a world reference in terms of cybersecurity certification;

㉘ – for these reasons, the Senate considers the predominant place envisaged for the ENISA in the cybersecurity certification process as unjustified. Indeed, it does not possess any expertise and could lead to a cybersecurity weakening within the Union, which runs counter to the objective of the current proposal;

㉙ – furthermore, Member States and National Supervisory Authorities on certification should closely preserve their legitimate place in the further European certification process and they should not be limited to a consultative role;

㉚ For these reasons, the Senate considers that the Regulation proposal COM (2017) 477 final does not comply with the subsidiarity principle.