Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2017/0225 (COD)

Brussels, 07 May 2018

WK 5420/2018 INIT

LIMITE

CYBER
TELECOM
CODEC
COPEN
COPS
COSI
CSC
CSCI
IND
JAI
JAIEX
POLMIL
RELEX

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Swedish delegation
To:	Horizontal Working Party on Cyber issues
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") - Comments from the Swedish delegation on recitals 13, 14, 15, 15a, 21, 54, 55a, 55e and 55f and Articles 7, 43, 46, 48 and 55

Delegations will find in Annex the comments of the Swedish delegation on recitals 13, 14, 15, 15a, 21, 54, 55a, 55e and 55f and Articles 7, 43, 46, 48 and 55 of the above mentioned proposal.

ANNEX

13. The Agency should assist the Commission by means of advice, opinions and analyses on all the Union matters related to policy and law development, update and review in the area of cybersecurity **and its sector-specific aspects in order to enhance relevance of EU policies and law with cybersecurity dimension and** ~~**ensure coherence**~~ ~~**enable**~~ **promote consistency in their implementation at national level**~~, including critical infrastructure protection and cyber resilience~~. The Agency should act as a reference point of advice and expertise for Union sector-specific policy and law initiatives where matters related to cybersecurity are involved.

Rationale: SE supports the role for ENISA in sector specific aspects. Nonetheless, enable consistency is better than "ensuring coherence" but ENISA's role should be to promote this. Ensuring and enable is a national responsibility.

14 The underlying task of the Agency is to promote the consistent implementation of the relevant legal framework, in particular the effective implementation of the NIS Directive, which is essential in order to increase cyber resilience. In view of the fast evolving cybersecurity threat landscape, it is clear that Member States must be supported by more comprehensive, cross-policy approach to building cyber resilience. However, this facilitation does not in any way deprive the Member States of their own responsibility to develop and maintain competences in the field of information security.

Rationale: ENISA's role should not in any way deprive each and every MS's responsibility to ensure a national competence in information security.

PUBLIC

15 The Agency should facilitate for ~~assist~~ the Member States and Union institutions, ~~**bodies, offices and**~~ agencies **and bodies** in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to ~~cyber~~security ~~problems~~ **threats** and incidents and in relation to the security of network and information systems. In particular, the Agency should support the development and enhancement of national CSIRTs, with a view of achieving a high common level of their maturity in the Union. **Activities carried out by ENISA relating to the operational capacities of Member States should be solely complementary to the own actions taken by Member States in order to fulfil their obligations arising from the NIS Directive and thus should not supersede them** ~~The Agency should also assist with the development and update of Union and Member States strategies on the security of network and information systems, in particular on cybersecurity, promote their dissemination and track progress of their implementation. The Agency should also offer trainings and training material to public bodies, and where appropriate "train the trainers" with a view to assisting Member States in developing their own training capabilities~~.

(15a) ~~**The Agency should also assist with the development and update of Union and upon request, Member States strategies on the security of network and information systems, in particular on cybersecurity, promote their dissemination and track progress of their implementation.**~~ **The Agency** ~~**should also**~~ **may offer trainings and training material to public bodies, and where appropriate "train the trainers" with a view to assisting Member States in developing their own training capabilities.**

PUBLIC

21 In compliance with its ~~operational~~ tasks **to support operational cooperation within the CSIRTs Network**, the Agency should be able to provide support to Member States **at their request**, such as by providing advice **on how to improve their capabilities to prevent, detect and respond to incidents, by assisting the** ~~or~~ technical **handling of incidents having a significant or substantial impact** ~~assistance~~, or **by** ensuring analyses of threats and incidents. **Assisting the technical handling of incidents having a significant or substantial impact includes ~~means~~ in particular that ENISA supports the voluntary sharing of technical solutions between Member States or produces combined technical information - such as technical solutions voluntarily shared by the Member States.** The Commission's Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises recommends that Member States cooperate in good faith and share amongst themselves and with ENISA information on large-scale cybersecurity incidents and crises without undue delay. Such information should further help ENISA in ~~performing its operational tasks~~ **supporting operational cooperation**.

New recital 54: All measures to be taken under the Regulation shall regard the principles of free movement of goods and services in the Treaty on the Functioning of the European Union and be non-discriminatory. This concerns in particular the preparation, adoption and application of standards and technical specification defining technical requirements and/or security evaluation methodology associated with a cyber security scheme

PUBLIC

(55a) The identification of technical specifications to be used in a European cybersecurity certification scheme should be carried out by respecting the principles laid down in Annex II of Regulation (EU) 1025/2012. Some deviations from these ~~principles~~ procedures could be however sometimes be allowed, in order to provide for a more flexible and less time-consuming way of working. ~~considered necessary in cases where those technical specifications are to be used in a European cybersecurity certification scheme referring to assurance level high.~~ In all circumstances the principles of transparency, openness, impartiality, consensus, effectiveness, relevance and coherence shall be applie while establishing such technical specifications

Rationale: An EU regulation cannot make general deviations from an existing EU regulation. Any such regulation must be defined in scope, and its purpose explained. Sweden thus proposes that

1) The second sentence in recital (55a) is deleted), 2) the wording of the second sentence is changed to "Some deviations from the procedures laid down there, could however sometimes be allowed in order to provide for a more flexible and less time-consuming way of working. In all circumstances the principles of transparency, openness, impartiality, consensus, effectiveness, relevance and coherence shall be applie while establishing such technical specifications"

PUBLIC

(55e)The manufacturer or provider of ICT products and services should keep the EU declaration of conformity and technical documentation of all relevant information relating to the conformity of the ICT products or services with a scheme at the disposal of the competent national cybersecurity certification authority in accordance with the procedure laid down in the European cybersecurity scheme ~~for 10 years~~. The technical documentation should specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the ICT product or service. The technical documentation should be so compiled to enable the assessment of the conformity of an ICT product or service with the relevant requirements.

Rationale: Flexibility needed: Sentence should read "…**scheme at the disposal of the competent national cybersecurity certification authority in accordance with the procedure laid down in the European cybersecurity scheme"**

(56f) When preparing a candidate scheme, ENISA should consult all relevant stakeholders, such as the European standardisation organisations, industrial organization, relevant national authorities, organisations based on mutual recognition agreements such as SOG-IS MRA, SMEs, consumer organisations as well as environmental and social stakeholders.

Rationale: Not only SMEs are relevant, therefore include "industrial organizations"

TITLE I GENERAL PROVISIONS

Article 7

~~Tasks relating to o~~ Operational cooperation at Union level

4. The Agency shall **support** ~~contribute to~~ the operational cooperation within the CSIRTs Network providing support to Member States **- at their request,** by:

(a) advising on how to improve their capabilities to prevent, detect and respond to incidents;

(b) ~~providing, at their request,~~ **~~assisting~~ facilitating the** technical **handling** ~~assistance in case~~ of incidents having a significant or substantial impact**, ~~including~~ in particular ~~facilitating~~ by supporting the voluntary sharing of technical solutions between Member States**;

Rationale: We still prefers that point c is deleted since it not only duplicates 7.4.b but also lower the level of incident or crisis. As a second, subordinate alternative, we prefer the alternative writing with both incident having a *significant or substantial impact* and with *in particular*, to show what it mainly is about and that it can not be any incident or crisis

PUBLIC

8. The Agency shall contribute to develop a cooperative response, at Union and Member States level, to large-scale cross-border incidents or crises related to cybersecurity, mainly by:

(c) ~~**supporting upon request of Member States, facilitating** the technical handling of an incident or crisis, including **facilitating by supporting** the **voluntary** sharing of technical solutions between Member States;~~ **ALTERNATIVE:** upon request of Member States, facilitating the technical handling of an incident having a significant or substantial impact, in particular by supporting the voluntary sharing of technical solutions between Member States

We still prefers that point c is deleted since it not only duplicates 7.4.b but also lower the level of incident or crisis. As a second, subordinate alternative, we prefer the alternative writing with both incident having a *significant or substantial impact* and with *in particular*, to show what it mainly is about and that it can not be any incident or crisis

PUBLIC

TITLE III

CYBERSECURITY CERTIFICATION FRAMEWORK

Article 43

European cybersecurity certification **framework ~~schemes~~**

1. The European cybersecurity certification framework is established in order to increase the level of security within the digital European Union. It sets governance that enables a harmonised approach at EU level of European cybersecurity certification scheme, in view of creating a digital single market for ICT processes, products and services. This regulation is without prejudice to the ability for the Member States to maintain or adopt national cybersecurity certification schemes for national security purposes, for example in the field of public procurement.

Rationale: There´s a need to clarify the right for MS to take actions regarding national security, especially regarding public procurement outside the defence sector. Therefore SE proposes an additional sentence. “This regulation is without prejudice to the ability for the Member States to maintain or adopt national cybersecurity certification schemes for national security purposes, for example in the field of public procurement”

PUBLIC

Article 46

Assurance levels of European cybersecurity certification schemes

2 The assurance levels basic, substantial and high shall ~~meet the following criteria respectively:~~ **refer to a certificate or an EU declaration of conformity issued in the context of a European cybersecurity certification scheme, which provides a corresponding degree of confidence (basic, substantial and/or high) in the claimed ~~or asserted~~ cybersecurity qualities of an ICT process, product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents as follows:**

c) **European cybersecurity certificate that refers to** assurance level **"**high**" ~~shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which~~** provides a **~~higher~~ high** degree of confidence in the claimed **~~or asserted~~** cybersecurity qualities of an ICT **process,** product or service **~~than certificates with the assurance level substantial, and is characterised with reference to technical specifications, standards~~ and ~~procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity~~ and in particular a confidence that cyber** incidents **can be prevented but there is also ability to resist state-of-the-art cyber attacks carried out by actors with significant and skilled ~~or unlimited~~ resources**.

Rationale: It is unrealistic that a product should be able to resist an attack with unlimited resources, change to "**significant and skilled ~~or unlimited~~ resources"**

Article 48

Cybersecurity certification

PUBLIC

4a. **In cases where a European cybersecurity certification scheme pursuant to Article 44 requires an assurance level high, the certificate should ~~can only~~ be issued by a national cybersecurity certification ~~supervisory~~ authority referred to in Article 50(1), in accordance with a decision in the certification scheme.**

Rationale: The practice that NCCA should issue high level certificates, should also be stated in the European cybersecurity scheme, for clarity. Thus the text should read:

In cases where a European cybersecurity certification scheme pursuant to Article 44 requires an assurance level high, the certificate should ~~can only~~ be issued by a national cybersecurity certification ~~supervisory~~ authority referred to in Article 50(1), in accordance with a decision in the certification scheme. 4b. By the way of derogation from paragraph 4a, ~~in duly justified cases~~ a particular European cybersecurity certification scheme may …

TITLE IV FINAL PROVISIONS

Article 55

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Rationale: Same content but more clarity. The text should read: Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

PUBLIC