Council of the
European Union

Brussels, 4 October 2018
(OR. en)

12799/18

LIMITE

CYBER 221
TELECOM 320
CODEC 1599
COPEN 334
COPS 352
COSI 213
CSC 284
CSCI 135
IND 270
JAI 964
JAIEX 126
POLMIL 153
RELEX 821

Interinstitutional File:
2017/0225(COD)

NOTE

From:	Presidency
To:	Delegations
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") - Debrief of the trilogue on 1 October 2018

I. INTRODUCTION

The objective of this note is to debrief delegations about the outcome of second trilogue, which was held on 1 October 2018 in Strasbourg and was dedicated to the certification part of the proposed Regulation. The first trilogue, dedicated to the ENISA part, was held on 14 September 2018, also in Strasbourg.

The trilogue was chaired by the chair of the ITRE Committee J. Buzek. The European Parliament was represented by the rapporteur Mrs A. Niebler as well as by shadow rapporteurs, Mr Danti (S&D), Tosenovský (ECR) , Mr P. Kouroumbashev (S&D) and Mr P. Telicka (ALDE). The Commission was represented by Commissioner M. Gabriel. The Council delegation was headed by the Deputy Permanent Representative T. Oberreiter.

The main aim of the meeting was to explain the position of both co-legislators on political issues identified in relation to the certification part of the Cybersecurity Act, and to explore possible areas of comprise. The Presidency approach was based on the mandate given by Coreper on 26 September 2018, as set out in 12489/18.

II. OUTCOME OF THE 2ND TRILOGUE

Both co-legislators explained their positions on six political issues as set out in the trilogue agenda and agreed to provide the Technical Meetings with a broad mandate to make progress on the whole regulation, wherever possible, and to identify possible areas of compromise, in view of the future trilogue meetings. The three Institutions expressed again their commitment to conclude the negotiations by the end of 2018.

The six political issues laid down in the agenda as regards the certification part were;

1. Governance of the European cybersecurity certification schemes

    1.1. Preparation, adoption and revision of a European cybersecurity certification scheme (Art. 44)

    1.2. Union rolling work programme (Art. 44.-1 EP)

    1.3. Involvement of the ECCG/Cybersecurity Members State Certification Group (Art. 44.2; 44.3 and 53.3.c)

    1.4. Stakeholder Certification Group (Art. 20a EP)

2. Certification schemes for operators of essential services (Art. 48a EP)

3. Peer review (Art. 50a EP+ 47.1.me CNS)

4. Information on certified products (Art. 47a EP)

5. Notification procedure (Art. 49.3a, 49.3b, 49.3c, 49.3d EP)

6. Evaluation and review (Art. 56) and Art. 56.2a (EP)

As a follow-up to the trilogue, a new technical meeting was organised on 2 October where the participants of the three Institutions agreed to a division of tasks and to submit new wording suggestions for the above mentioned Articles. The Presidency will submit its suggestions first for discussion to the HWP on Cyber Issues on 9 October 2018. These suggestions will then be discussed at a technical meeting on 12 October 2018.

The following issues were discussed:

1. Governance of the European cybersecurity certification schemes

1.1. Preparation, adoption and revision of a European cybersecurity certification scheme (Art. 44)

At five preparatory technical meetings, the governance of the cybersecurity schemes was divided in five phases (planning, request, preparation, adoption and review of the schemes) in order to make the entire process more visible and structured. Considering the complexity of the certification framework, the Presidency saw merit in following this division in phases and advocated to concentrate the discussions on a number of basic principles in relation to each of these phases. The Parliament however focused the discussions on two of its main demands: the establishment of a Union Rolling Work Programme (RWP) and the creation of a Stakeholder Certification Group.

1.2. Union rolling work programme (Art. 44.-1 EP)

The Presidency defended the Council's position as set out in 12489/18 and stated that it could consider the inclusion of a RWP subject to the following four conditions:

- it should be a legally non-binding instrument e.g. staff working document,

- the European Cybersecurity Certification Group (ECCG) should have the possibility for direct request to ENISA without limitations as laid down in Art. 53(3)(c) Council,

- the ECCG should have the possibility to take part in the public consultation prior to the RWP by issuing an opinion which Commission has to consider.

- there should be a guaranteed involvement of all stakeholders, including SME and consumers by an open, transparent and inclusive consultation process prion to the publication of the RWP by the Commission.

Also the Commission was in favour of a RWP as a non binding instrument and considered that the Commission should be able to submit a direct request to ENISA to prepare a scheme in case of urgency or on the basis of market needs.

The European Parliament wanted the RWP to be a binding document but showed flexibility on the instrument for adoption since it agreed that a delegated act could be too burdensome for the RWP. It insisted, however, on the fact that the Stakeholder Certification Group would have the same powers as the ECCG in the entire certification framework, including submitting a direct request to ENISA. The Parliament had some legal questions on the possibility for the ECCG to submit a direct request to ENISA to prepare a scheme which would be examined by the Legal Services of the three Institutions.

It was agreed that the technical meetings should explore a compromise wording including an explicit debate of the Legal Services.

1.3. Involvement of the ECCG/Cybersecurity Members State Certification Group (Art. 44.2 44.3 and 53.3.c)

The Presidency underlined the specificity and the importance of the involvement of Member States in the context of the certification framework taking into account 1) the long-standing expertise of Member States and the high level of trust which schemes operated or endorsed by national authorities are enjoying; and 2) that the major part which Member States and their authorities will play the enforcement of the adopted schemes.

The Parliament opposed the Council's text which foresees that the ECCG shall adopt an opinion on the candidate scheme which ENISA "shall take utmost account of" before transmitting the scheme to the Commission. The Parliament views this as a veto right for the Member States.

The Presidency clarified that the opinion of the ECCG is not a veto and that the absence of an opinion would not block the process. The Presidency stressed that the possibility for the EECG to ask ENISA directly and without limitations to prepare a candidate scheme remained a very strong point for the Council. Furthermore the Presidency recalled that the composition and the level of the Member States' delegation remained a Member State competence and that therefore this reference was deleted in Art. 53 (2).

1.4. Stakeholder Certification Group (Art. 20a EP)

The Presidency pointed out that the Council also attaches great importance to an involvement of all stakeholders which is ensured throughout the Council's text (e.g. Art. 53 in conjunction with Art. 44 (1a)) and by the possibility of creating ad hoc working groups as set out in Art. 19 (4).

The Presidency took note of the Parliament's suggestion for a new article on the so-called Stakeholder Certification Group which the Council did not support since more clarifications were needed regarding the equal representation of stakeholders in the SCG, its relation with other groups such as the Permanent Stakeholders' Group pursuant to Art. 20 as well as to other similar groups (e.g. ECSO) and the composition and selection process of the SCG. The Presidency underlined that this group should only have an advisory task but should not be able to request for a scheme.

The Commission also asked for clarifications regarding the composition and powers of the SCG as well as possible repercussions on ENISA's resources.

The Parliament underlined that that the SCG was an important element to the EP's position which in its opinion should be appropriately reflected in the text. The Parliament even went further and stated that the SCG should be placed at equal footing with the ECCG throughout the entire process ("mirroring the ECCG").

The technical meetings were tasked to discuss a compromise wording regarding Article 44 and the related Articles 20a EP and 53. The advise of the Legal Services would also be sought.

2. Certification schemes for operators of essential services (Art. 48a EP)

The Presidency explained the Council's legal concerns on the implications of the Parliament's amendment, the interference with the NIS Directive and the security concerns which might arise since the proposed obligation for operators of essential services could even lead to lowering the cybersecurity level among these operators.

It was agreed that further discussions should take place at technical level together with the Legal Services of the three Institutions.

3. Peer review (Art. 50a EP+ 47.1.me CNS)

Both co-legislators agreed to introduce the concept of peer review which would be a safeguard to "certification shopping". Differences remained in relation to the scope, addressees and level of detail. The Parliament introduced a new Article 50a with a wide scope whereas the Council text (Art. 47 (1)(me)) limits it to bodies issuing the certificates for assurance level "high".

The technical meeting was tasked to elaborate a compromise wording taking into account existing regimes for the Conformity assessment bodies under Accreditation regulation (EC) No 765/2008.

4. Information on certified products (Art. 47a EP)

The Parliament briefly presented its suggestion for a new Art. 47a on Cybersecurity information for certified products, process and services. The Presidency acknowledged that this provision could represent an added value since information on certified product would help in raising awareness of the end users and building consumer trust. On the other hand the Presidency considered the wording of the article is very prescriptive and stated that it could lead to possible additional burdens and requirements for the industry and might also overburden the consumers.

The technical meeting was tasked to elaborate a compromise wording allowing for more flexibility.

5. Notification procedure (Art. 49.3a, 49.3b, 49.3c, 49.3d EP)

The Presidency took note of the amendments suggested by the Parliament in Art. 49 which aim at avoiding fragmentation of the internal market. The Presidency was willing to consider certain elements as long as there would be no interference with the sovereignty of Member States and their competences and enough flexibility and less formality would be granted.

The technical meeting was tasked to elaborate a compromise wording.

6. Evaluation and review (Art. 56) and Article 56.2a (EP)

The Parliament still advocated a review period of two years whereas at technical level an agreement seemed to exist to have a review no later than five years. The Presidency, supported by the Commission, expressed its surprise and called on the Parliament to re-consider this topic and produce a four-column table for the next meeting.

The technical meeting was tasked to elaborate a compromise wording.

III. NEXT STEPS

- The Presidency will debrief COREPER I on 5 October 2018 and HWP on Cyber Issues on 9 October.
- HWP on Cyber Issues meeting on 9, 23 (poss.) and 30 (poss.) October 2018 to discuss some technical proposals.
- Technical meetings will be held on 12, 18 and 24 October 2018 (tbc).