Council of the European Union
General Secretariat

Interinstitutional files:
2017/0225 (COD)

Brussels, 07 May 2018

WK 5456/2018 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:	Finnish 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 Finnish delegation on recitals 19, 21, 23, 27, 55f, 56c, 57, 59, 60, 62 and Articles 7, 44, 47, 47a, 48, 50, 53, 54 and 58

Delegations will find in Annex the comments of the Finnish delegation on recitals 19, 21, 23, 27, 55f, 56c, 57, 59, 60, 62 and Articles 7, 44, 47, 47a, 48, 50, 53, 54 and 58 on the above mentioned proposal.

ANNEX

General remarks:

We would like to thank the Presidency for the hard and good work on the proposal. We think that in many ways the text is moving to the right direction. We are happy to see that the creation of Digital Single Market for ICT products and services has been embraced as the objective of the proposed European cybersecurity certification framework. However, we still think that the text could be improved to let this objective to shine through. We should ensure that in the future there is more secure and safe ICT products and services for the use of all the Europeans. It is also important to increase the visibility of the digital security of these products and services to make sure that the users can choose the ones most suitable to their needs.

To create a well-functioning certification framework, we must keep in mind not to create unnecessary bureaucracy and make sure that all the member states can equally participate the process. We should leave enough flexibility for the member states to organise the activities of the national authorities in the best suitable manner. The system should be easily accessible to the industry and transparent.

Comments on the proposed text:

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "~~*EU Cybersecurity*~~ *European Union* Agency *for Cybersecurity*", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

RECITALS:

Recital 19: FI proposes a change of text as following:

(19) The Agency should support the **~~to the greatest extent possible~~** ~~to an EU level~~ response ~~in case~~ of the Member States of large-scale cross-border cyber security incidents and crises. This function should **be performed in accordance with an approach to be agreed by Member States in the context of the Commission Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises and limited to the competencies that are in accordance to this regulation. It could** include gathering relevant information and acting as facilitator between the CSIRTs Network and the technical community as well as decision makers responsible for crisis management. Furthermore, the Agency could support the handling of incidents from a technical perspective by facilitating relevant technical exchange of solutions between Member States and by providing input into public communications. The Agency should support the process by testing modalities of such cooperation through ~~yearly~~ **regular** cybersecurity exercises.

Rationale:

It would be important to emphasize that the ENISA's competencies and mandate is defined in the Cyber Security Act and its activities in the area of EU level response in case of large-scale cross-border cyber security incidents are limited to these competencies.

Recital 21: FI agrees that the incident handling in the light of this regulation should be limited to sharing information between the member states. More operational tasks should be left to the member states' responsibility. FI supports the proposed changes to the text as following:

(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 shall mean** ~~**includes**~~ **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**.

Recital 23: FI proposes a change of text as following:

(23) **The support by the Agency to e**~~E~~x-post technical **inquiries** ~~**enquiries**~~ ~~into~~ **of** incidents with significant impact ~~in more than one Member State supported or undertaken by the Agency~~ upon request ~~or with the agreement of the concerned~~ **on the** Member States **concerned** should be focused on the prevention of future incidents ~~and be carried out without prejudice to any judicial or administrative proceedings to apportion blame or liability~~. ~~**The Member States concerned should provide the necessary information in order to enable the Agency to effectively support the technical enquiry. The provision of such information should be carried out without prejudice to Article 346 of the Treaty on the Functioning of the European Union or other public policy reasons.**~~

Rationale:

FI believes that the recitals in this act should not introduce new obligations to the Member States. This regulation covers the tasks of ENISA not the obligations of the member states. If the recital text is not meant to create new obligations, a reference to the Treaty text is unnecessary.

Recital 27: FI proposes a change of text as following:

(27) In order to increase the resilience of the Union, the Agency should develop excellence on the subject of **cyber** security of [digital] **infrastructures supporting in particular the sectors listed in Annex II of the NIS Directive and those used by the digital service providers listed in Annex III of that Directive** ~~internet infrastructure and of the critical infrastructures~~, by providing advice, guidance and best practices. With a view to ensuring easier access to better structured information on cybersecurity risks and potential remedies, the Agency should develop and maintain the "information hub" of the Union, a one-stop-shop portal providing the public with information on cybersecurity deriving from the EU and national institutions, agencies and bodies.

Rationale:

There is no need to ENISA to develop excellence on the subject of security of infrastructures supporting the sectors listed in NIS directive. This would, for example, refer to security of road network or airports. ENISA should focus its activities on the security of digital infrastructure or cyber security of the infrastructure.

Recital 55 f: FI proposes a change of text and adding a new recital as following:

(55f) Member States or interested stakeholder organisations should be entitled to propose either to the Commission or to the European Cybersecurity Certification Group the preparation of a candidate scheme. Interested stakeholder organisations are industry or consumer representatives' organisations, including representatives of SMEs organisations that have a valid interest in the development of a particular European cybersecurity certification scheme. ~~Such proposals should be examined in light of the criteria developed by the European Cybersecurity Certification Group by virtue of guidelines~~

(new) To ensure the transparency of the preparation of the schemes the Commission and the Group should keep a public record of the proposals made to them by the industry or member states. The record could include general details about the entity that made the proposal and the type of the certification scheme proposed. To make sure that all the proposals are handled in equal and transparent manner the Commission and the Group should publish common principles on assessing the proposals based on transparency, openness, impartiality, effectiveness, relevance and coherence. The principles should also cover the co-operation of the Group and the commission on assessing the proposals avoiding the duplication of activities.

Rationale: see our proposal on article 44.

Recital 56 c: FI proposes a change of text as following:

(56c) When preparing a candidate scheme, ENISA should consult all relevant stakeholders, such as the industry, European standardisation organisations, 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: FI would like to see the industry included in the list.

Recital 57: FI proposes a change of text as following:

(57) Recourse to European cybersecurity certification **and EU declaration of conformity** should remain voluntary, unless otherwise provided in Union or national legislation **adopted in accordance with Union law. In the absence of harmonised legislation, Member States may adopt national technical regulations in accordance with Directive (EU) 2015/1535 providing for mandatory certification under a European cybersecurity certification scheme. Member States could also use the recourse to European cybersecurity certification in the context of public procurement and Directive 2014/14/EU**. **All national measures should be taken respecting the EU treaties, particularly the free movement of goods and services.**

Rationale: FI would prefer a specific reference to the EU treaties to make sure that there would be no temptation to use the national law to create fragmentation on internal market or barriers to the free movement of products and services.

Recital 59: FI proposes a change of text as following:

(59) It is necessary to require all Member States to designate ~~one~~ cybersecurity certification **~~supervisory~~** authority to supervise compliance **with obligations arising from this Regulation. The tasks of the authority can be given to a single or more authorities. If the member state finds it appropriate the tasks can be given also to one or more existing authorities. authority should in particular monitor and enforce the obligations of the manufacturer or provider of ICT products and services established in their respective territories relating to the EU declaration of conformity, assist the national accreditation bodies in the monitoring and supervision of activities of conformity assessment bodies, authorise conformity assessment bodies to carry out its tasks when they meet additional requirements set out in a scheme and monitor relevant developments in the field of cybersecurity certification ~~of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory with the requirements of this Regulation and of the relevant cybersecurity certification schemes~~**. National **cybersecurity** certification **~~supervisory~~** authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by **them ~~conformity assessment bodies established in their territories~~**, investigate to the extent appropriate the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable time period. Moreover, they should cooperate with other national **cybersecurity** certification **~~supervisory~~** authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.

Rationale: To make sure that all the member states can equally participate the process, we should leave enough flexibility for the member states to organise the activities of the national authorities in the best suitable manner.

Recital 60: FI proposes a change of text as following:

(60) With a view to ensuring the consistent application of the European cybersecurity certification framework, a European Cybersecurity Certification Group (the 'Group') consisting of national **cybersecurity** certification ~~**supervisory**~~ authorities **or other representatives appointed by the member states** should be established. The main tasks of the Group should be to advise and assist the Commission in its work to ensure a consistent implementation and application of the European cybersecurity certification framework; to assist and closely cooperate with the Agency in the preparation of candidate cybersecurity certification schemes; recommend that the Commission request the Agency to prepare a candidate European cybersecurity certification scheme; and to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

Rationale: FI argues that it should be left to the Member states to decide how they are represented in the Group.The change in the text would make it also possible to establish the group with no delay after the adoption of this regulation and before the member states have designated the national supervisory authority. Designating the national supervisory authority may require legislative changes in the member states.

Recital 62: FI support deletion of this recital:

~~(62) The Agency's support to cybersecurity certification should also include liaising with the Council Security Committee and the relevant national body, regarding the cryptographic approval of products to be used in classified networks.~~

New Recital on peer-review: FI proposes an addition of a new recital on peer-review if the concept is kept in the regulation.

(new) A European cybersecurity certification scheme may include rules concerning peer review mechanism for the bodies issuing European cybersecurity certificates for high assurance levels. Peer review should be viewed as a mutual learning process that helps to build trust between Member States. The meaning of the peer-review process should be to build confidence in certificates issued and ensure high quality and transparency of the certification process. Participation in peer review mechanism shall be voluntary and results of the peer review should always have a non-binding character.

COMMENTS TO THE ARTICLES:

Article 7: FI proposes a change of text as following:

Article 7

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

1. The Agency shall support operational cooperation among **Member States, Union institutions, agencies and** ~~competent public~~ bodies, and between stakeholders.

2. The Agency shall cooperate at operational level and establish synergies with Union institutions, **~~bodies, offices and~~** agencies **and bodies**, including the CERT-EU, those services dealing with cybercrime and supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern, including:

   (a) the exchange of know-how and best practices;

   (b) the provision of advice and guidelines on relevant issues related to cybersecurity;

   (c) the establishment, upon consultation of the Commission, of practical arrangements for the execution of specific tasks.

3. The Agency shall provide the secretariat of the CSIRTs network, pursuant to Article 12(2) of Directive (EU) 2016/1148 ~~and **in this capacity** shall actively facilitate the information sharing and the cooperation among its members~~.

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** ~~facilitating by~~ **supporting the voluntary sharing of technical solutions between Member States**;

~~(c) analysing vulnerabilities, artefacts and incidents;~~

(ca) upon request by the Member States concerned providing support to ex-post technical ~~enquiries~~ **inquiries of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148.**

In performing these tasks, the Agency and CERT-EU shall engage in a structured cooperation in order to benefit from synergies **and avoid duplication of activities**~~, in particular regarding operational aspects~~.

~~5. Upon a request by two or more Member States concerned, and with the sole purpose of providing advice for the prevention of future incidents, the Agency shall provide support to or carry out an ex-post technical enquiry following notifications by affected undertakings of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148. The Agency shall also carry out such an enquiry upon a duly justified request from the Commission in agreement with the concerned Member States in case of such incidents affecting more than two Member States.~~

~~The scope of the enquiry and the procedure to be followed in conducting such enquiry shall be agreed by the concerned Member States and the Agency and is without prejudice to any on-going criminal investigation concerning the same incident. The enquiry shall be concluded by a final technical report compiled by the Agency in particular on the basis of information and comments provided by the concerned Member States and undertaking(s) and agreed with the concerned Member States. A summary of the report focussing on the recommendations for the prevention of future incidents will be shared with the CSIRTs network.~~

6. The Agency shall organise **regular** ~~annual~~ cybersecurity exercises at Union level, and support Member States and EU institutions, agencies and bodies in organising exercises following their request(s). **Such exercises at Union level may include technical, operational or strategic elements** ~~Annual exercises at Union level shall include technical, operational and strategic elements and help to prepare the cooperative response at the Union level to large-scale cross-border cybersecurity incidents~~. **Once every two years, a large-scale exercise shall be organised that will have all that elements.** The Agency shall also contribute to and help organise, where appropriate, sectoral cybersecurity exercises together with relevant ~~ISACs and permit ISACs to~~ **organisations that may** participate also **in** ~~to~~ Union level cybersecurity exercises.

7. The Agency shall**, in close cooperation with Member States,** prepare a regular EU Cybersecurity Technical Situation Report on incidents and threats based on open source information, its own analysis, and reports shared by, among others: Member States' CSIRTs ~~(on a voluntary basis)~~ or NIS Directive Single Points of Contact (**both on a voluntary basis** ~~in accordance with NIS Directive Article 14 (5)~~); European Cybercrime Centre (EC3) at Europol, CERT-EU.

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:

   (a) aggregating reports from national sources **shared on a voluntary basis** with a view to contribute to establishing common situational awareness;

   (b) ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs Network and the technical and political decision-makers at Union level;

   (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~~;

(d) supporting **EU institutions, agencies and bodies and, upon request, Member States in the** public communication around the incident or crisis;

(e) **supporting Member States, at their request, to** testing the cooperation plans to respond to such incidents or crises.

Rationale: FI agrees that the incident handling in the light of this regulation should be limited to sharing information between the member states (art 7(4)b and art 7(8)c). More operative tasks should be left to the member states' responsibility.

TITLE III
CYBERSECURITY CERTIFICATION FRAMEWORK

Article 44: FI proposes a change of text as following:

Article 44

Preparation and adoption of a European cybersecurity certification scheme

1. Following a request from the Commission or the Group, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation.

1a. The preparation of a candidate European cybersecurity certification scheme may be proposed to the Commission or the Group by Member States or interested stakeholder organisations. The Commission and the Group should keep a public record of the proposals and publish common principles on assessing the proposals.

2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders **by transparent consultation processes** and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice ~~required by ENISA~~ in relation to the preparation of the candidate scheme **and adopt an opinion on the candidate scheme before its submission to the Commission, ~~including by providing opinions~~** ~~where necessary~~. **ENISA shall ensure that the candidate schemes are consistent with ~~meets the requirements of~~ the applicable harmonised standard used for accreditation of the conformity assessment body.**

3. ENISA shall **take utmost account of the opinion of the Group before transmitting ~~transmit~~** the candidate ~~European cybersecurity certification~~ scheme prepared in accordance with paragraph 2 of this Article to the Commission **~~along with the remarks or reservations made by the Group members~~**.

4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(2), providing for European cybersecurity certification schemes for ICT **processes,** products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.

Rationale:

FI welcomes the presidency's new approach to the article. Neverteless the process could be further streamlined. This would be important to make the system more attractive and as accessible as possible to the industry but at the same time ensure the transparency of the process. To reach that aim FI proposes changes to the proposed para 1a. According these changes **the industry could propose the preparation of the certification scheme to both the Commission and the Group.** A public record should be kept of the proposals made. This would be important to improve **the transparency**. The record could include general details about the entity that made the proposal and the type of the certification scheme proposed.

In addition, FI proposes that instead of the Group adopting guidelines on the assessment of the proposal, the Commission and the Group should publish common principles on handling and assessing he proposals made to them. The meaning of these principles would be to ensure that the process is fair, equal and transparent. The principles should also cover the co-operation of the Group and the commission on assessing the proposals avoiding the duplication of activities.

Article 47: FI proposes a change of text as following:

Article 47

Elements of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall include **at least** the following elements:

(a) subject-matter and scope of the certification **scheme**, including the type or categories of ICT **processes,** products and services covered **as well as an elaboration of how the certification scheme suits the needs of the expected target groups**;

(b) ~~detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by~~ reference to ~~Union or~~ international**, European, national** standards or technical specifications **where standards are not available, followed in the evaluation**;

(c) where applicable, one or more assurance levels;

(ca) where applicable, specific or additional requirements applicable to conformity assessment bodies in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(d) specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45**~~, and that specific cybersecurity requirements referred to in point (b)~~** are achieved;

(e) **where applicable,** information to be supplied **or otherwise be made available** to the conformity assessment bodies by an applicant which is necessary for certification;

(f) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(g) ~~where surveillance is part of the scheme, the~~ rules for monitoring compliance with the requirements of the certificates **or the EU declaration of conformity**, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;

(h) **where applicable,** conditions for granting **and renewing a certificate**, **as well as** maintaining, continuing, ~~**renewing,**~~ extending and reducing the scope of certification;

rules concerning the consequences of non-conformity of certified **or self-assessed** ICT products and services with the ~~certification~~ requirements **of the scheme**;

(i) rules concerning how previously undetected cybersecurity vulnerabilities in ICT **processes,** products and services are to be reported and dealt with;

(j) **where applicable,** rules concerning the retention of records by conformity assessment bodies;

(k) identification of national **or international** cybersecurity certification schemes covering the same type or categories of ICT **processes,** products and services**, security requirements and evaluation criteria and methods**;

(l) the content of the issued certificate **or the EU declaration of conformity;**

(ma) maximum period of validity of certificates, if applicable;

(mb) disclosure policy for granted, amended and withdrawn certificates;

(mc) conditions for the mutual recognition of certification schemes with third countries;

[(md) where applicable, rules concerning a non-binding and voluntary peer review mechanism for the bodies issuing European cybersecurity certificates for high assurance levels pursuant to Article 48(4a) ~~and (4b)~~.]

2. The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.

3. Where a specific Union act so provides, certification **or the EU declaration of conformity** under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that act.

4. In the absence of harmonised Union legislation, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

Rationale: It is very important to FI that the obligations and tasks of national authorities are defined in the regulation. To respect the principle of foreseeability no new possible binding and compulsory systems involving the national authorities and which rules would be only created in the certification scheme given as implementing act should be created in the regulation. Peer-review, if introduced, should always be voluntary and non-binding.

Article 47 a: FI would prefer a specific reference to the treaty text in paragraph 3 to make sure that there would be no temptation to use the national law to create fragmentation on internal market or barriers to the free movement of products and services:

Article 47a

Conformity self-assessment

1. A European cybersecurity certification scheme may allow for carrying out a conformity assessment under the sole responsibility of the manufacturer or provider of ICT products and services. Such conformity assessment shall be applicable only to ICT products and services of low risk and complexity corresponding to assurance level basic.

~~Article 47b~~

~~EU declaration of conformity~~

~~2~~1. **The manufacturer or provider of ICT products and services may issue an EU declaration of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By drawing up such a declaration, the manufacturer or provider of ICT products and services shall assume responsibility for the compliance of the ICT product or service with the requirements set out in the scheme.**

~~3~~2. **The manufacturer or provider of ICT products and services shall 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 national cybersecurity certification ~~supervisory~~ authority referred to in Article 50(1) for 10 years. A copy of the EU declaration of conformity shall be submitted to the national cybersecurity certification ~~supervisory~~ authority and to ENISA.**

~~4~~3. **The issuing of EU declaration of conformity is voluntary unless otherwise specified in the Union law or in Member States law.**

5. The EU declaration of conformity issued pursuant to this Article shall be recognised in all Member States.

Article 48: FI supports the deletion of proposed additions for paragraphs 4a and 4b. The derogation on paragraph 4 is sufficient to in certain duly justified cases to limit who can issue the certificates. If not possible to delete the paragraph 4a from the text, FI proposes to change the text as following and delete paragraph 4b:

Article 48

Cybersecurity certification

1. ICT **processes,** products and services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 44 shall be presumed to be compliant with the requirements of such scheme.

2. The certification shall be voluntary, unless otherwise specified in Union law **or in Member States law**.

3. A European cybersecurity certificate pursuant to this Article **referring to assurance level basic or substantial** shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44.

4. By ~~**the**~~ way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity **certification** scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such public body shall be one of the following:

(a) a national **cybersecurity** certification ~~**supervisory**~~ authority referred to in Article 50(1);

(b) a **public** body that is accredited as conformity assessment body pursuant to Article 51(1) ~~**or**~~

~~**(c) a body established under laws, statutory instruments, or other official administrative procedures of a Member State concerned and meeting the requirements for bodies certifying products, processes and services further to ISO/IEC 17065:2012**~~.

[4a. **In cases where a European cybersecurity certification scheme pursuant to Article 44 requires an assurance level high, the certificate can only be issued by a national cybersecurity certification ~~supervisory~~ authority referred to in Article 50(1) or by a conformity assessment body referred to in Article 51:**

(a) upon prior approval by a national cybersecurity certification authority for each individual certificate issued by a conformity assessment body; or

(b) upon prior general delegation of this task to a conformity assessment body by the national cybersecurity certification authority.

~~**4b. By the way of derogation from paragraph 4a, in duly justified cases a particular European cybersecurity certification scheme may provide that a European cybersecurity certificate for assurance level high resulting from that scheme may be issued by a conformity assessment body referred to in Article 51:**~~

~~**(a) upon prior approval by a national cybersecurity certification authority for each individual certificate issued by a conformity assessment body; or**~~

~~**(b) upon prior general delegation of this task to a conformity assessment body by the national cybersecurity certification authority.**~~ **]**

5. The natural or legal person which submits its ICT **processes,** products or services to the certification mechanism shall ~~**provide**~~ **make available to** the conformity assessment body referred to in Article 51 ~~**with**~~ all information necessary to conduct the certification procedure.

5a. The holder of a certificate shall inform the body issuing the certificate about any later detected irregularities concerning the security of the certified ICT process, product or service that may affect the certificate. The body shall forward this information without undue delay to the national cybersecurity certification authority.

6. Certificates shall be issued for ~~a maximum period of three years~~ **the period defined by the particular certification scheme** and may be renewed, ~~**under the same conditions,**~~ provided that the relevant requirements continue to be met.

7. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.

Rationale: To avoid unnecessary bureaucracy and ensuring enough flexibility also considering the certification schemes of assurance level high, CAB should be able under certain conditions issue also the High Level certificates by default. If the text in para 4a would be changed according to FI proposal there would still be the opportunity to limit the issuance of a certificate only to a public body in duly justified cases according paragraph 4.

Article 50: FI proposes a change of text as following:

Article 50

National cybersecurity certification ~~supervisory~~ authorities

1. Each Member State shall appoint a national **cybersecurity** certification **~~supervisory~~** authority.

2. Each Member State shall inform the Commission of the identity of the authority appointed.

3. **Without prejudice to Article 48(4)(a) ~~and (c)~~,** ~~E~~each national **cybersecurity** certification **~~supervisory~~** authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise.

3a. Member States shall ensure that the activities of the national cybersecurity certification authority related to the issuance of certificates in accordance with article 48(4)(a) adhere to a strict separation of roles and responsibilities with the supervisory activities in this article and that both activities function independently from each other.

4. Member States shall ensure that national **cybersecurity** certification **~~supervisory~~** authorities have adequate resources to exercise their powers and to carry out, in an effective and efficient manner, the tasks assigned to them.

5. For the effective implementation of the regulation, it is appropriate that these authorities participate in the European Cybersecurity Certification Group established pursuant to Article 53 in an active, effective, efficient and secure manner.

6. National **cybersecurity** certification ~~**supervisory**~~ authorities shall:

~~(a) monitor and enforce the application of the provisions under this Title at national level and supervise compliance of the certificates that have been issued by conformity assessment bodies established in their respective territories with the requirements set out in this Title and in the corresponding European cybersecurity certification scheme;~~

(aa) monitor and enforce the obligations of the manufacturer or provider of ICT products and services set out in Article 47a(2) and (3) ~~established in their respective territories~~ b;

~~**monitor and supervise, in close cooperation with**~~ **assist the national accreditation bodies in the monitoring and supervision of, ~~the~~** activities of conformity assessment bodies for the purpose of this Regulation~~**, including in relation to the notification of conformity assessment bodies and the related tasks set out in Article 52 of this Regulation. These monitoring and supervisory activities shall not overlap with the activities performed by the national accreditation bodies**~~;

(ba) monitor and supervise the activities of the ~~public body~~ bodies referred to in Article 48(4)~~(c)~~;

(bb) authorise conformity assessment bodies referred to in Article 51(1ba) and restrict, suspend or withdraw existing authorisation in cases of non-compliance with the requirements of this Regulation;

(b) handle complaints lodged by natural or legal persons in relation to certificates issued by ~~**conformity assessment bodies or public bodies referred to**~~ **the national cybersecurity certification authority in accordance with Article 48(4)~~(a) established in their territories~~**, investigate, to the extent appropriate, the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation within a reasonable time period;

(c) cooperate with other national **cybersecurity** certification ~~**supervisory**~~ authorities or other public authorities, including by sharing information on possible non-compliance of ICT **processes,** products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;

(d) monitor relevant developments in the field of cybersecurity certification.

7. Each national **cybersecurity** certification ~~**supervisory**~~ authority shall have at least the following powers:

(a) to request conformity assessment bodies**,** ~~**and**~~ European cybersecurity certificate holders **and issuers of EU declaration of conformity** to provide any information it requires for the performance of its task;

(b) to carry out investigations, in the form of audits, of conformity assessment bodies**,** ~~**and**~~ European cybersecurity certificates' holders **and issuers of EU declaration of conformity**, for the purpose of verifying compliance with the provisions under Title III;

(c) to take appropriate measures, in accordance with national law, in order to ensure that conformity assessment bodies**,** ~~**or**~~ certificate holders **and issuers of EU declaration of conformity** comply with this Regulation or with a European cybersecurity certification scheme;

(d) to obtain access to any premises of conformity assessment bodies and European cybersecurity certificates' holders for the purpose of carrying out investigations in accordance with Union or Member State procedural law;

(e) to withdraw, in accordance with national law, certificates **issued by the national cybersecurity certification authority in accordance with Article 48(4)(a)** that are not compliant with this Regulation or a European cybersecurity certification scheme;

(f) to impose penalties, as provided for in Article 54, in accordance with national law, and to require the immediate cessation of the breaches of obligations set out in this Regulation.

(New) The tasks of the supervisory authority according this article are limited to the **issuers of EU declaration of conformity established in their respective territories.**

8. National **cybersecurity** certification ~~**supervisory**~~ authorities shall cooperate amongst each other and the Commission and, in particular, exchange information, experiences and good practices as regards cybersecurity certification and technical issues concerning cybersecurity of ICT **processes,** products and services.

Rationale: As it in now unclear how the requirement in para 6 relates to para 7 FI proposes to add a new paragraph to clarify that the tasks of the national authority only concern the issuers of EU declaration of Conformity established in their respective territory.

Article 53: FI proposes a change of text as following:

Article 53

European Cybersecurity Certification Group

1. The European Cybersecurity Certification Group (the 'Group') shall be established.

2. The Group shall be composed of national **cybersecurity** certification ~~**supervisory**~~ authorities. The authorities shall be represented by the heads or by other high level representatives of national **cybersecurity** certification ~~**supervisory**~~ authorities.

3. The Group shall have the following tasks:

(a) to advise and assist the Commission in its work to ensure a consistent implementation and application of the present Title, in particular regarding cybersecurity certification policy issues, coordination of policy approaches, and the preparation of European cybersecurity certification schemes;

(b) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme in accordance with Article 44 of this Regulation;

(ba) to adopt an opinion on the candidate scheme pursuant to Article 44 of this Regulation;

to ~~propose to the Commission that it requests~~ **request** the Agency to prepare a candidate European cybersecurity certification scheme in accordance with Article 44 of this Regulation;

~~**(ca) to develop and adopt guidelines on criteria for assessment of proposals for the preparation of a candidate scheme submitted to the Commission or the Group pursuant to Article 44(1a);**~~

(c) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;

(d) to examine the relevant developments in the field of cybersecurity certification and exchange good practices on cybersecurity certification schemes;

(e) to facilitate the cooperation between national **cybersecurity** certification ~~**supervisory**~~ authorities under this Title through **capacity building,** the exchange of information, in particular by establishing methods for the efficient exchange of information relating to all issues concerning cybersecurity certification**;**

(fa) to ~~participate in the organisation and~~ provide support ~~to the implementation of~~ the peer review mechanism ~~between the bodies referred to in Article 48(4a) and (4b)~~ established in accordance with ~~the rules established in~~ the European cybersecurity certification scheme pursuant to Article 47(1)(md) of this Regulation.

4. The Commission shall chair the Group **in the capacity of a moderator** and provide the secretariat to it, with the assistance of ENISA as provided for in Article 8(a).

Rationale: see article 44 and article 47. As the characteristics of the peer-review will be defined in more detail in the certification schemes themselves and as they may vary the Group can be obligated to only support the mechanism.

Article 54: FI supports the Commission's proposal to leave the rules on the penalties to be laid down by the member states. No EU-level harmonisation is needed.

Article 54

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Title and European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall [by …/without delay] notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.

Article 58: FI supports that an efficient transposition period is secured considering articles requiring legislative activities in Member States. These articles include at least art 50, 52, 53a, 53 b and 54.

Article 58

Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. This Regulation shall be binding in its entirety and directly applicable in all Member States.