European Distribution System Operators for Smart Grids

EDSO amendments to the Proposal for a Regulation on ENISA and on Information and Communication Technology cybersecurity certification

March 2018

Amendment proposals

Article 43
European cybersecurity certification schemes

ORIGINAL TEXT	*PROPOSED TEXT*
A European cybersecurity certification scheme shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist ***at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems.***	**A 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 certification, in view of creating a digital single market for secured ICT products, systems and services.** **The framework enables the adoption of ~~A~~** European cybersecurity certification schemes **that** shall attest that the ICT products**, processes** and services**,** that have been certified in accordance with such scheme comply with specified **security** requirements **and properties** as regards their ability to resist. **~~at a given level of assurance., actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems.~~** **Member States may adopt or maintain national certification schemes for national security purposes, requiring other or additional security measures from the EU schemes. Those national schemes shall not be affected by this regulation.**

Justification:

This amendment places this initiative under the umbrella of the Digital Single Market. Moreover, it leaves Member States room for improvement in areas that relate to national security purposes.

Article 44

Preparation and adoption of a European Cybersecurity Certification Scheme

ORIGINAL TEXT	*PROPOSED TEXT*
1. ***Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation.*** Member States ***or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission***. 2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders 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, including by providing opinions ***where necessary***. 3. ENISA shall transmit the candidate ***European cybersecurity certification*** scheme prepared in accordance with paragraph 2 of this Article to the Commission. 4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation. 5. ENISA shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes.	~~1. Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation.~~ **The preparation of a candidate European cybersecurity certification scheme may be proposed to the Commission or to the European Cybersecurity Certification Group (the 'Group') established under Article 53 by,** Member States**,** ~~**or the European Cybersecurity Certification Group (the 'Group') established under Article 53**~~ **or an industry representatives body.**~~**may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.**~~ **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.** 2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders 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, including by providing opinions ~~**where necessary**~~. 3. **Upon the approval of the candidate European cybersecurity certification scheme by the Group,** ENISA shall transmit the candidate ~~**European cybersecurity certification**~~ scheme prepared in accordance with paragraph 2 of this Article to the Commission. 4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in

	accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46, and 47 of this Regulation. 5. ENISA shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification scheme.

Justification:

Member States may identify some certification needs as crucial for their national security. Moreover, the European industry has shown great interest, conducted a wide array of projects and successfully implemented good practices in the area of cybersecurity certification.

Therefore, this amendment proposes a role for Member States and industrial user representatives in proposing candidate certification schemes to the Commission.

Considering national experience in this field, this amendment also proposes to give the Group a more active role and provide guidance to ENISA.

Article 45

Security objectives of European cybersecurity certification schemes

ORIGINAL TEXT	*PROPOSED TEXT*
A European cybersecurity certification scheme shall be so designed to take into account, as applicable, the following security objectives: (a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure;	A European cybersecurity certification scheme shall be so designed **as** to take into account, as applicable, **at least** the following security objectives: (a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure;
(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss or alteration;	(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss or alteration;
(c) ensure that authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;	(c) ensure that authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;

(d) record which data, functions or services have been communicated, at what times and by whom; (e) ensure that it is possible to check which data, services or functions have been accessed or used, at what times and by whom; (f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident; (g) ensure that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates.	(d) record which data, functions or services have been communicated, at what times and by whom; (e) ensure that it is possible to check which data, services or functions have been accessed or used, at what times and by whom; (f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident; (g) ensure that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates**;** **(h) ensure that ICT products and services are developed according to the security requirements stated in the particular scheme.**

Justification:

This amendment aims to reinforce certification schemes, make them more robust by ensuring the effective implementation of the scheme in products and services.

Article 46

Assurance levels of European cybersecurity certification schemes

ORIGINAL TEXT	*PROPOSED TEXT*
1. A European cybersecurity certification scheme may specify one or more of the following assurance levels: basic, substantial and/or high, for ***ICT products and services*** issued under that scheme. 2. The assurance levels basic, substantial and high shall ***meet the following criteria respectively***: (a) ***assurance level basic shall*** refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a ***limited*** degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto,	1. A European cybersecurity certification scheme may specify **at least** one or more of the following assurance levels: basic, substantial and/or high, for **cybersecurity certificates** ~~**ICT products and services**~~ issued under that scheme. 2. The assurance levels basic, substantial and high shall ~~**meet the following criteria respectively:**~~ ~~**(a) assurance level basic shall**~~ refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a ~~**limited**~~ **corresponding** degree of confidence **(basic, substantial and/or high)** in the claimed or asserted cybersecurity qualities of an ICT product or service,

including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents; ***(b) assurance level substantial shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of an ICT 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 substantially the risk of cybersecurity incidents;*** ***(c) assurance level high shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT 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 incidents.***	and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to **substiantly** decrease the risk of**, or to prevent** cybersecurity incidents.; **depending on the respective assurance level of the certificate to be issued, the adequate evaluation method shall be based on ~~a~~the following methodology:** **(a) technical review by a conformity assessment body of the technical documentation of the ICT product or service;** **(b) verification by the conformity assessment body of the conformity of security functionalities of the product or service to its technical documentation;** **(c) efficiency testing by the conformity assessment body, which assesses the resistance of the security functionalities against attackers having significant capacities.** **~~(b) assurance level substantial shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of an ICT 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 substantially the risk of cybersecurity incidents;~~** **~~(c) assurance level high shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT 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 incidents.~~

Justification:

While keeping the three levels of assurance, this article aims to ensure that the adequate elements are tested in the elaboration of certification schemes.

Article 47
Elements of European cybersecurity certification schemes

ORIGINAL TEXT	*PROPOSED TEXT*
1. ***A*** European cybersecurity certification scheme ***shall include the following elements***: (a) subject-matter and scope of the certification, including the type or categories of ICT products and services covered; (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 standards or technical specifications; (c) where applicable, one or more assurance levels; (d) specific evaluation criteria and methods ***used,*** including types of evaluation, in order to demonstrate that the specific ***objectives referred to in Article 45*** are achieved; ***(e)*** information to be supplied 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, including mechanisms to	1. **Technical elements shall be considered when preparing a** ~~**A**~~ European cybersecurity certification scheme**, an indicative list of which is** ~~**shall include the following elements:**~~ (a) subject-matter and scope of the certification **scheme**, including the type or categories of ICT products and services covered; (b) ~~**detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by**~~ reference to**,** ~~**Union**~~ **European** or international **or national** standards or technical specifications **followed in the evaluation and certification process**; (c) where applicable, one or more assurance levels; (d) specific evaluation criteria and methods **referred to in Article 46 (2) (a, b, c,)** ~~**used**~~**,** including types of evaluation, in order to demonstrate that the specific **cybersecurity** ~~**objectives referred to in Article 45, and that specific**~~ **requirements referred to in Art. 45** ~~**point (hb)**~~ are achieved; ~~(d)~~(e) **where applicable, specific or additional requirements applicable to conformity assessment bodies**; (f) information to be supplied to the conformity assessment bodies by an

demonstrate the continued compliance with the specified cybersecurity requirements; (h) conditions for granting, maintaining, continuing, extending and reducing the scope of certification; (i) rules concerning the consequences of non-conformity of certified ICT products and services with the certification requirements; (j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with; (k) rules concerning the retention of records by conformity assessment bodies; (l) identification of national cybersecurity certification schemes covering the same type or categories of ICT products and services; (m) the content of the issued certificate. 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 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.	applicant which is necessary for certification; (g) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used; (h) ~~**where surveillance is part of the scheme, the**~~ rules for monitoring compliance with the requirements of the certificates, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements; (i) conditions for granting, maintaining, continuing, **renewing,** extending and reducing the scope of certification; (j) rules concerning the consequences of non-conformity of certified ICT products and services with the certification requirements **of the scheme**; (k) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with; (l) rules concerning the retention of records by conformity assessment bodies; (m) identification of national **or international** cybersecurity certification schemes covering the same type or categories of ICT products and services, **security requirements and evaluation criteria and methods;**, (n) the content of the issued certificate; (o) **maximum period of validity of certificates, if applicable;** (p) **disclosure policy for granted, amended and withdrawn certificates**;

	(q) **governance mechanism for updates, amendments and coordination for any particular certification scheme**. 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 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.

Justification:

This amendment proposes a more comprehensive list of technical elements to be included in the certification scheme.

Article 48
Cybersecurity certification

ORIGINAL TEXT	*PROPOSED TEXT*
1. ICT 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. 3. A European cybersecurity certificate pursuant to this Article 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 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 certification supervisory authority referred to in Article 50(1) ***(b) a 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. 5. The natural or legal person which submits its ICT products or services to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure. 6. Certificates shall be issued for ***a maximum period of three years*** and may	1. ICT 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 EU Member States' law.** 3. A European cybersecurity certificate pursuant to this Article **for assurance level basic and substantial as referred to in Article 46 (2),** 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. **A European cybersecurity certificate pursuant to this Article for assurance level high as referred to in Article 46 (2), can only be issued by a national certification supervisory authority referred to in Article 50 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 certification supervisory authority referred to in Article 50(1) ~~**(b) a body that is accredited as conformity assessment body pursuant to Article 51(1) or**~~ ~~**(c)**~~**(b)** a body established under laws, statutory instruments, or other official administrative procedures of a Member State concerned and meeting the requirements for bodies certifying

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.	products, processes and services further to ISO/IEC 17065:2012. 5. The natural or legal person which submits its ICT products or services to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure. 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.

Justification:

This amendment aims to increase the effectiveness of certification schemes by ensuring that schemes aiming to ensure a high level of cybersecurity will be issued by national certification supervisory authorities.

It also provides for more flexible periods of validity, to be defined for each scheme instead of three years for each schemes.

Article 49

National cybersecurity certification schemes and certificate

ORIGINAL TEXT	*PROPOSED TEXT*
1. Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant Article 44(4). ***Existing n***ational cybersecurity certification schemes and the related procedures for the ICT products and services not covered by a European cybersecurity certification scheme shall continue to exist.	1. Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant Article 44(4). ~~**Existing n**~~**N**ational cybersecurity certification schemes and the related procedures for the ICT products and services not covered by a European cybersecurity certification scheme**, as**

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products and services covered by a European cybersecurity certification scheme in force. 3. Existing certificates issued under national cybersecurity certification schemes shall remain valid until their expiry date.	**defined in article 43,** shall continue to exist. 2. Member States shall not introduce new national cybersecurity certification schemes for ICT products and services covered by a European cybersecurity certification scheme in force. 3. Existing certificates issued under national cybersecurity certification schemes **and covered by a European cybersecurity certification scheme** shall remain valid until their expiry date.

Justification:

As Members States may have various needs and capacities in terms of services and products, national cybersecurity certification schemes Member States should stay in force in areas that are not covered by European schemes.

Article 50
National certification supervisory authorities

ORIGINAL TEXT	*PROPOSED TEXT*
1. Each Member State shall appoint a national certification supervisory authority. 2. Each Member State shall inform the Commission of the identity of the authority appointed. 3. Each national certification supervisory authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise. 4. Member States shall ensure that national 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	1. Each Member State shall appoint a national certification supervisory authority. 2. Each Member State shall inform the Commission of the identity of the authority appointed. 3. Each national certification supervisory authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise. 4. Member States shall ensure that national 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 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; (b) monitor and supervise 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; ***(c)*** handle complaints lodged by natural or legal persons in relation to certificates issued by 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; ***(d)*** cooperate with other national certification supervisory authorities or other public authorities, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific European cybersecurity certification schemes; ***(e)*** monitor relevant developments in the field of cybersecurity certification. 7. Each national certification supervisory authority shall have at least the following powers: (a) to request conformity assessment bodies and European cybersecurity certificate holders to provide any information it requires for the performance of its task;	active, effective, efficient and secure manner. 6. National 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; (b) monitor and supervise 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; **(c) monitor and supervise the activities of the public body referred to in article 48 (4) (c)** ~~(c)~~**(d)** handle complaints lodged by natural or legal persons in relation to certificates issued by 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; ~~(d)~~**(e)** cooperate with other national certification supervisory authorities or other public authorities, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific European cybersecurity certification schemes; ~~(e)~~**(f)** monitor relevant developments in the field of cybersecurity certification. 7. Each national certification supervisory authority shall have at least the following powers: (a) to request conformity assessment bodies and European cybersecurity

(b) to carry out investigations, in the form of audits, of conformity assessment bodies and European cybersecurity certificates' holders, 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 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 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. 8. National 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 products and services.	certificate holders 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, 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 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 that are not compliant with this Regulation or a European cybersecurity certification scheme; **(f) to withdraw licensing of conformity assessment bodies, as referred to in article 51 (2), that do not comply with this regulation;** **(g)** 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. 8. National 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 products and services. **9. National certification supervisory authorities can offer mutual support to**

	share ressources on certification activities.

Justification:

This amendment aims to provide a wider role to national certification supervisory authorities.

Article 51
Conformity assessment bodies

ORIGINAL TEXT	*PROPOSED TEXT*
1. The conformity assessment bodies shall be accredited by the national accreditation body named pursuant to Regulation (EC) No 765/2008 only when they meet the requirements set out in the Annex to this Regulation. ***2***. Accreditation shall be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements set out in this Article. Accreditation bodies shall revoke an accreditation of a conformity assessment body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation	1. The conformity assessment bodies shall be accredited by the national accreditation body named pursuant to Regulation (EC) No 765/2008 only when they meet the requirements set out in the Annex to this Regulation. **The requirements shall be defined in accordance with global accreditation standards and shall ensure that the accreditation bodies operate in open, transparent, and fair manner.** **2. Beyond and without prejudice to the scope of paragraph 1, for evaluation methods pursuant to Article 46 (2) (b, c), a European cybersecurity certification scheme shall provide specific additional requirements referred to in Article 47 (1) (e) for the conformity assessment body. Prior to performing evaluations, conformity assessment bodies shall, in addition to their accreditation, be licensed by the national certification supervisory authority, only if the specific additional requirements laid out in the European cybersecurity certification scheme are met.** ~~2~~.3 Accreditation shall be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements set out in this Article. Accreditation bodies shall revoke an accreditation of a conformity assessment body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer,

	met or where actions taken by a conformity assessment body infringe this Regulation.

Justification:

This amendment aims to provide a more thorough assessment of conformity assessment bodies that could be led by national certification supervisory authorities. It also ensures that each certification scheme establishes the right requirements for it to be efficient.

Article 53
European Cybersecurity Certification Group

ORIGINAL TEXT	*PROPOSED TEXT*
1. The European Cybersecurity Certification Group (the 'Group') shall be established. 2. The Group shall be composed of national certification supervisory authorities. The authorities shall be represented by the heads or by other high level representatives of national 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; (c) to ***propose to the Commission that it*** requests the Agency to prepare a candidate European cybersecurity certification scheme in accordance with Article 44 of this Regulation; (d) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes; (e) to examine the relevant developments in the field of cybersecurity certification	1. The European Cybersecurity Certification Group (the 'Group') shall be established. 2. The Group shall be composed of national certification supervisory authorities. The authorities shall be represented by the heads or by other high level representatives of national 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; (c) to ~~**propose to the Commission that it**~~ requests the Agency to prepare a candidate European cybersecurity certification scheme in accordance with Article 44 of this Regulation; (d) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;

and exchange good practices on cybersecurity certification schemes; (f) to facilitate the cooperation between national certification supervisory authorities under this Title through the exchange of information, in particular by establishing methods for the efficient exchange of information relating to all issues concerning cybersecurity certification. 4. The Commission shall chair the Group and provide the secretariat to it, with the assistance of ENISA as provided for in Article 8(a).	(e) to examine the relevant developments in the field of cybersecurity certification and exchange good practices on cybersecurity certification schemes; (f) to facilitate the cooperation between national certification supervisory authorities under this Title through the exchange of information, in particular by establishing methods for the efficient exchange of information relating to all issues concerning cybersecurity certification. **(g) to support capacity building within the EU through cooperation between EU NCSAs.** **(i) to arrange the peer reviewing process of the public bodies mentioned in article 48(4). This process aims at validating, at EU level, which public bodies, as referred to in article 48(4), are competent to deliver high level certificates;** **(j) based on the results of the peer reviewing process, to decide on the list of public bodies, as referred to in article 48.4, able to deliver high level certificates ;** 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).

Justification:

This amendment aims to enhance the activities of this Group that will gather the skilled experts in cybersecurity certification. The Group should assess the capacity of certification bodies to issue the highest quality and technical expertise.

EDSO
for smart grids

EDSO for Smart Grids is a European association gathering leading electricity distribution system operators (DSOs), cooperating to bring smart grids from vision to reality.
www.edsoforsmartgrids.eu