**DRAFT REPORT**

on the 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")

(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Committee on Industry, Research and Energy

Rapporteur: Angelika Niebler

Rapporteur for the opinion (*):
Nicola Danti, Committee on the Internal Market and Consumer Protection

(*) Associated committee – Rule 54 of the Rules of Procedure
Symbols for procedures

* Consultation procedure
*** Consent procedure
****I Ordinary legislative procedure (first reading)
****II Ordinary legislative procedure (second reading)
****III Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in **bold italics** in the left-hand column. Replacements are indicated in **bold italics** in both columns. New text is indicated in **bold italics** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in **bold italics**. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in **bold italics** and by deleting or striking out the text that has been replaced.

By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.
## CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION</td>
</tr>
<tr>
<td>EXPLANATORY STATEMENT</td>
</tr>
</tbody>
</table>
DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION


(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2017)0477),

– having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C8-0310/2017),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Economic and Social Committee of 14 February 2018¹,

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the reasoned opinion submitted, within the framework of Protocol No 2 on the application of the principles of subsidiarity and proportionality, by the French Senate, asserting that the draft legislative act does not comply with the principle of subsidiarity,

– having regard to the report of the Committee on Industry, Research and Energy and the opinions of the Committee on the Internal Market and Consumer Protection, the Committee on Foreign Affairs, the Committee on Budgets and the Committee on Civil Liberties, Justice and Home Affairs (A8-0000/2018),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

¹ OJ C xx of ..., p. xx.
Amendment 1

Proposal for a regulation
Recital 13

Text proposed by the Commission

(13) The Agency should assist the Commission by means of advice, opinions and analyses on all the Union matters related to policy and law development, update and review in the area of cybersecurity, including critical infrastructure protection and cyber resilience. The Agency should act as a reference point of advice and expertise for Union sector-specific policy and law initiatives where matters related to cybersecurity are involved.

Amendment

(13) The Agency should assist the Commission by means of advice, opinions and analyses on all the Union matters related to policy and law development, update and review in the area of cybersecurity, including critical infrastructure protection and cyber resilience. The Agency should act as a reference point of advice and expertise for Union sector-specific policy and law initiatives where matters related to cybersecurity are involved. Its expertise will be especially needed when preparing the Union’s multiannual work programme for European cybersecurity certification schemes.

Or. en

Amendment 2

Proposal for a regulation
Recital 19

Text proposed by the Commission

(19) The Agency should contribute to an EU level response in case of large-scale cross-border cybersecurity incidents and crises. This function should 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

Amendment

(19) The Agency should contribute to an EU level response in case of large-scale cross-border cybersecurity incidents and crises. This function should 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 cybersecurity exercises. The Agency should respect the competences of the Member States regarding cybersecurity, especially those concerning public security, defence, national security and the activities of the state in areas of criminal law.

Amendment 3
Proposal for a regulation
Recital 25

Text proposed by the Commission
(25) Member States may invite undertakings concerned by the incident to cooperate by providing necessary information and assistance to the Agency without prejudice to their right to protect commercially sensitive information.

Amendment
(25) Member States may invite undertakings concerned by the incident to cooperate by providing necessary information and assistance to the Agency without prejudice to their right to protect commercially sensitive information and information relevant to public security.

Amendment 4
Proposal for a regulation
Recital 30

Text proposed by the Commission
(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational

Amendment
(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational
management of large-scale IT systems (eu-LISA), European Aviation Safety Agency (EASA) and any other EU Agency that is involved in cybersecurity. It should also liaise with authorities dealing with data protection in order to exchange know-how and best practices and provide advice on cybersecurity aspects that might have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the Agency’s Permanent Stakeholders Group. In liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks.

Amendment 5
Proposal for a regulation
Recital 33

Text proposed by the Commission

(33) The Agency should further develop and maintain its expertise on cybersecurity certification with a view to supporting the Union policy in this field. The Agency should promote the uptake of cybersecurity certification within the Union, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthening trust in the digital internal market.

Amendment

(33) The Agency should further develop and maintain its expertise on cybersecurity certification with a view to supporting the Union policy in this field. The Agency should build upon existing best practices and promote the uptake of cybersecurity certification within the Union, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthening trust in the digital internal market.
Amendment 6
Proposal for a regulation
Recital 35

Text proposed by the Commission

(35) The Agency should encourage Member States and service providers to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal cybersecurity. In particular, service providers and product manufacturers should withdraw or recycle products and services that do not meet cybersecurity standards. In cooperation with competent authorities, ENISA may disseminate information regarding the level of cybersecurity of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the security, including cybersecurity, of their products and services.

Amendment

(35) The Agency should encourage Member States and service providers to raise their general security standards, in particular by providing necessary updates so that all internet users can take the necessary steps to ensure their own personal cybersecurity. In particular, service providers and product manufacturers should withdraw or recycle products and services that do not meet cybersecurity standards. In cooperation with competent authorities, ENISA may disseminate information regarding the level of cybersecurity of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the security, including cybersecurity, of their products and services.

Or. en

Amendment 7
Proposal for a regulation
Recital 36

Text proposed by the Commission

(36) The Agency should take full account of the ongoing research, development and technological assessment activities, in particular those carried out by the various Union research initiatives to advise the Union institutions, bodies, offices and agencies and where relevant, the Member States, at their request, on

Amendment

(36) The Agency should take full account of the ongoing research, development and technological assessment activities, in particular those carried out by the various Union research initiatives to advise the Union institutions, bodies, offices and agencies and where relevant, the Member States, at their request, on
research needs in the area of network and information security, in particular cybersecurity. More specifically, a cooperation with the European Research Council (ERC) and the European Institute for Innovation and Technology (EIT) should be established and security research should be included in the Ninth Research Framework Programme (FP9) and Horizon 2020.

Amendment 8
Proposal for a regulation
Recital 44

Text proposed by the Commission

(44) The Agency should have a Permanent Stakeholders’ Group as an advisory body, to ensure regular dialogue with the private sector, consumers’ organisations and other relevant stakeholders. The Permanent Stakeholders’ Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the attention of the Agency. The composition of the Permanent Stakeholders Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure sufficient representation of stakeholders in the work of the Agency.

Amendment

(44) The Agency should have a Permanent Stakeholders’ Group as an advisory body, to ensure regular dialogue with the private sector, consumers’ organisations and other relevant stakeholders. The Permanent Stakeholders’ Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the attention of the Agency. To ensure a better involvement of the relevant stakeholders in the certification process, the Permanent Stakeholder Group should have the right to propose the preparation of a candidate European cybersecurity certification scheme to the Commission and the European Cybersecurity Certification Group (the 'Group') and should also be consulted in the further process. The composition of the Permanent Stakeholders’ Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure sufficient representation of stakeholders in the work of the Agency.
Amendment 9

Proposal for a regulation

Recital 47

Text proposed by the Commission

(47) Conformity assessment is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. For the purposes of this Regulation, certification should be considered as a type of conformity assessment regarding the cybersecurity features of a product, process, service, system, or a combination of those ("ICT products and services") by an independent third party, other than the product manufacturer or service provider. Certification cannot guarantee per se that certified ICT products and services are cyber secure. It is rather a procedure and technical methodology to attest that ICT products and services have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example as specified in technical standards.

Amendment

(47) Conformity assessment is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. For the purposes of this Regulation, certification and self-assessment should be considered as a type of conformity assessment regarding the cybersecurity features of a product, process, service, system, or a combination of those ("ICT products and services") by an independent third party, other than the product manufacturer or service provider. Self-assessment may be undertaken by the product manufacturer or service provider, as foreseen in and according to the New Legislative Framework\(^a\) and specified in this Regulation. Certification cannot guarantee per se that certified ICT products and services are cyber secure. It is rather a procedure and technical methodology to attest that ICT products and services have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example as specified in technical standards.


Or. en

Amendment 10

Proposal for a regulation
Recital 50

Text proposed by the Commission

(50) Currently, the cybersecurity certification of ICT products and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In this context, a certificate issued by one national cybersecurity authority is not in principle recognised by other Member States. Companies thus may have to certify their products and services in several Member States where they operate, for example with a view to participating in national procurement procedures. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach with regard to horizontal cybersecurity issues, for instance in the field of the Internet of Things. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual utilisation.

Amendment

(50) Currently, the cybersecurity certification of ICT products and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In this context, a certificate issued by one national cybersecurity authority is not in principle recognised by other Member States. Companies thus may have to certify their products and services in several Member States where they operate, for example with a view to participating in national procurement procedures. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach with regard to horizontal cybersecurity issues, for instance in the field of the Internet of Things. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual utilisation. A risk-based approach is required whilst acknowledging that a one-size-fits-all approach is not possible.
Amendment 11
Proposal for a regulation
Recital 53

Text proposed by the Commission

(53) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products and services. These schemes should be implemented and supervised by national certification supervisory authorities and certificates issued within these schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or other private organisations should fall outside the scope of the Regulation. However, the bodies operating such schemes may propose to the Commission to consider such schemes as a basis for approving them as a European scheme.

Amendment

(53) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products and services. These schemes should be implemented and supervised by national certification supervisory authorities and certificates issued within these schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or other private organisations should fall outside the scope of the Regulation. However, the bodies operating such schemes may propose to the Commission to consider such schemes as a basis for approving them as a European scheme. The Agency should identify and assess the schemes already operated by the industry or private organisations in order to choose best practices which could become part of a European scheme.

Amendment 12
Proposal for a regulation
Recital 56

Text proposed by the Commission

(56) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services. The Commission, based on the candidate scheme proposed by ENISA, should then be empowered to

Amendment

(56) The Commission or the Group should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services. The Commission, based on the candidate scheme proposed by ENISA, should then be empowered to
adopt the European cybersecurity certification scheme by means of implementing acts. Taking account of the general purpose and security objectives identified in this Regulation, European cybersecurity certification schemes adopted by the Commission should specify a minimum set of elements concerning the subject-matter, the scope and functioning of the individual scheme. These should include among others the scope and object of the cybersecurity certification, including the categories of ICT products and services covered, the detailed specification of the cybersecurity requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods, as well as the intended level of assurance: basic, substantial and/or high.

The assurance level shall depend on the risk resulting from the context and intended use of the ICT product, process and service.

Or. en

Amendment 13

Proposal for a regulation
Recital 57

Text proposed by the Commission

(57) Recourse to European cybersecurity certification should remain voluntary, unless otherwise provided in Union or national legislation. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act. Moreover,

Amendment

(57) Recourse to European cybersecurity certification should remain voluntary for assurance levels basic and substantial but not for ICT products, processes and services with assurance level high. At a later stage, and depending on the maturity of implementation in the Member States and the criticality of a product or a service, it is recognised that potentially mandatory schemes for all ICT products and services may begin to evolve in a phased approach. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the
Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme.

internal market, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act. Moreover, Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme.

---

**Amendment 14**

Proposal for a regulation

Recital 57 a (new)

*Text proposed by the Commission*

(57 a) A duty to issue a product declaration containing structured information in respect of the certification of the product, process or service is introduced to provide the consumer with more information and to allow the consumer to make a well-founded choice.

*Amendment*

Or. en

**Amendment 15**

Proposal for a regulation

Recital 58

*Text proposed by the Commission*

(58) Once a European cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services should be able to submit an
application for certification of their products or services to a conformity assessment body of their choice. Conformity assessment bodies should be accredited by an accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should 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. Accreditation bodies should revoke an accreditation of a conformity assessment body 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. 

Audits shall be carried out to ensure that an equivalent level of quality, know-how and expertise applies in the Union, the results of which shall be reported to ENISA and the Group.

Or. en

Amendment 16
Proposal for a regulation
Article 1 – paragraph 1 – introductory part

Text proposed by the Commission

With a view to ensuring the proper functioning of the internal market while aiming at a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation:

Amendment

With a view to ensuring the proper functioning of the internal market by avoiding a fragmentation of certification schemes in the Union, while aiming at a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation:

Or. en

Justification

This emphasises the need to achieve harmonisation with the cybersecurity framework and to avoid duplication and fragmentation across Member States
Amendment 17

Proposal for a regulation
Article 1 – paragraph 1 – point b

_text proposed by the Commission_

(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products and services in the Union. Such framework shall apply without prejudice to specific provisions regarding voluntary or mandatory certification in other Union acts.

_amendment_

(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products, processes, and services in the Union. Such framework shall apply without prejudice to specific provisions regarding voluntary and, if and where appropriate, mandatory certification in other Union acts.

_or. en_

Justification

-Inclusion of ‘process’ in the scope of the Regulation: with the inclusion of processes, the whole product lifecycle is covered and secured. -Voluntary nature: This emphasises the voluntary nature of the scheme - a voluntary certification scheme is the rule and mandatory certification will apply only exceptionally and under strict conditions.

Amendment 18

Proposal for a regulation
Article 1 – paragraph 1 a (new)

_text proposed by the Commission_

The objectives and the tasks of the Agency shall be without prejudice to the competences of the Member States regarding cybersecurity, and in any case, without prejudice to activities concerning public security, defence, national security and the activities of the state in areas of criminal law.

_amendment_

Or. en
Justification

By moving this exclusion from Art. 3 to Art. 1 of the Regulation, it is made clear that the competences of the Member States are safeguarded for the whole framework regulation.

Amendment 19

Proposal for a regulation

Article 2 – paragraph 1 – point 8

Text proposed by the Commission

(8) ‘cyber threat’ means any potential circumstance or event that may adversely impact network and information systems, their users and affected persons.

Amendment

(8) ‘cyber threat’ means any potential circumstance or event that may damage, disrupt or otherwise adversely impact network and information systems, their users and affected persons.

Or. en

Justification

Clarification of the definition

Amendment 20

Proposal for a regulation

Article 2 – paragraph 1 – point 9

Text proposed by the Commission

(9) ‘European cybersecurity certification scheme’ means the comprehensive set of rules, technical requirements, standards and procedures defined at Union level applying to the certification of Information and Communication Technology (ICT) products and services falling under the scope of that specific scheme;

Amendment

(9) ‘European cybersecurity certification scheme’ means the comprehensive set of rules, technical requirements, standards and procedures defined at Union level and according to international and European standards approved by ENISA, applying to the certification of Information and Communication Technology (ICT) products, processes and services falling under the scope of that specific scheme;

Or. en
Amendment 21

Proposal for a regulation
Article 2 – paragraph 1 – point 10

Text proposed by the Commission

(10) ‘European cybersecurity certificate’ means a document issued by a conformity assessment body attesting that a given ICT product or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;

Amendment

(10) ‘European cybersecurity certificate’ means a document issued either by a conformity assessment body or by self-assessment from the manufacturer, where provided for in this Regulation, attesting that a given ICT product, process or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;

Or. en

Justification

This amendment allows self-assessment and aligns it to the New Legislative Framework

Amendment 22

Proposal for a regulation
Article 2 – paragraph 1 – point 11 a (new)

Text proposed by the Commission

(11 a) ‘ICT process’ means any set of activities performed to design, develop, maintain and deliver an ICT product or service;

Amendment

(11 a) ‘ICT process’ means any set of activities performed to design, develop, maintain and deliver an ICT product or service;

Or. en

Amendment 23

Proposal for a regulation
Article 2 – paragraph 1 – point 16 a (new)

Text proposed by the Commission

(16 a) ‘national certification supervisory authority’ means a body appointed by

Amendment

(16 a) ‘national certification supervisory authority’ means a body appointed by
each Member State in accordance with Article 50 of this Regulation;

Amendment 24

Proposal for a regulation
Article 2 – paragraph 1 – point 16 b (new)

Text proposed by the Commission

(16 b) ‘self-assessment’ means the statement by which the manufacturer demonstrates that specific requirements relating to products, processes and services have been fulfilled;

Amendment

Justification

This definition is needed to align it to the New Legislative Framework

Amendment 25

Proposal for a regulation
Article 3 – paragraph 1

Text proposed by the Commission

1. The Agency shall undertake the tasks assigned to it by this Regulation for the purpose of contributing to a high level of cybersecurity within the Union.

Amendment

1. The Agency shall undertake the tasks assigned to it by this Regulation and shall be reinforced for the purpose of contributing to a high level of cybersecurity within the Union and to ensure consistency by taking into account the Member States’ cooperation achievements under the NIS Directive.

Justification

Clarification that structures are already in place which this Regulation aims to reinforce
Amendment 26
Proposal for a regulation
Article 3 – paragraph 3

Text proposed by the Commission

3. The objectives and the tasks of the Agency shall be without prejudice to the competences of the Member States regarding cybersecurity, and in any case, without prejudice to activities concerning public security, defence, national security and the activities of the state in areas of criminal law.

Amendment

deleted

Or. en

Justification

The paragraph should be moved to Art. 1 (2) instead

Amendment 27
Proposal for a regulation
Article 4 – paragraph 3

Text proposed by the Commission

3. The Agency shall support capacity building and preparedness across the Union, by assisting the Union, Member States and public and private stakeholders in order to increase the protection of their network and information systems, develop skills and competencies in the field of cybersecurity, and achieve cyber resilience.

Amendment

3. The Agency shall support capacity building and preparedness across the Union by assisting the Union institutions, agencies and bodies, Member States and public and private stakeholders in order to increase the protection of their network and information systems, develop and improve cyber resilience and response capacities, raise awareness and develop skills and competencies in the field of cybersecurity.

Or. en
Amendment 28
Proposal for a regulation
Article 4 – paragraph 5

Text proposed by the Commission

5. The Agency shall increase cybersecurity capabilities at Union level in order to complement the action of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents.

Amendment

5. The Agency shall contribute to increasing cybersecurity capabilities at Union level in order to complement the action of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents.

Or. en

Amendment 29
Proposal for a regulation
Article 4 – paragraph 6

Text proposed by the Commission

6. The Agency shall promote the use of certification, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthen trust in the digital internal market.

Amendment

6. The Agency shall promote the use of certification with a view to avoiding fragmentation in the internal market and improving its functioning, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthen trust in the digital internal market, as well as increasing the compatibility between existing national and international certification schemes.

Or. en

Amendment 30
Proposal for a regulation
Article 6 – paragraph 1 – point g
Text proposed by the Commission

Amendment

(g) the Member States by organising yearly large-scale cybersecurity exercises at the Union level referred to in Article 7(6) and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them;

(g) the Member States by organising regular large-scale cybersecurity exercises at the Union level referred to in Article 7(6) and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them;

Or. en

Justification

Having in mind the level of complexity, the number of people involved in this exercise and the need for debriefings after the exercise, a yearly rhythm is not realistic. The amendment will allow to achieve a comprehensive exercise with an added value.

Amendment 31

Proposal for a regulation
Article 6 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1 a. The Agency shall facilitate the establishment and launch of a long-term European IT security project to further foster cybersecurity research in the Union and the Member States, in cooperation with the European Research Council (ERC) and the European Institute of Innovation and Technology (EIT) and with regard to Union’s research programmes.

Or. en

Justification

The security research needs to be further developed. This can be done by requesting a close cooperation with the relevant agency and institutes and by linking it to the Framework Programme 9 and Horizon 2020.
Amendment 32

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission

1. The Agency shall support operational cooperation among competent public bodies, and between stakeholders.

Amendment

1. The Agency shall support operational cooperation among Member States, Union institutions, agencies and bodies, and between stakeholders, with a view to achieving collaboration, by analysing and assessing existing national-level schemes, by developing and implementing a plan and by using the appropriate instruments to achieve the highest level of cybersecurity certification in the Union and the Member States.

Or. en

Justification

This framework Regulation should be seen as a starting point and the choice between harmonisation and mutual recognition will follow at a later stage. The Agency is best suited to do this leverage exercise.

Amendment 33

Proposal for a regulation
Article 7 – paragraph 4 – subparagraph 1 – point b

Text proposed by the Commission

(b) providing, at their request, technical assistance in case of incidents having a significant or substantial impact;

Amendment

(b) providing, at their request, technical assistance in the form of information sharing and expertise in case of incidents having a significant or substantial impact;

Or. en

Justification

“technical assistance” is a very wide and uncertain notion. It can be understood as a mere exchange of information and reach until the transfer of technical data. It needs to be made clear that domains of national competence are not infringed when significant incidents are concerned (see Art. 1 (2) and therefore be limited. Clear exclusion of too far-reaching
transfer of technical data.

Amendment 34

Proposal for a regulation
Article 7 – paragraph 4 – subparagraph 1 – point b a (new)

Text proposed by the Commission

(b a) Where a situation requires urgent action, a Member State may request the assistance of experts from the Agency to assess the situation. The request shall include a description of the situation, the possible aims and envisaged needs.

Amendment

Or. en

Justification

A procedure should be added for the event requiring a rapid and European wide intervention.

Amendment 35

Proposal for a regulation
Article 7 – paragraph 5 – subparagraph 1

Text proposed by the Commission

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.

Amendment

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. In so doing, ENISA shall make sure not to disclose the actions taken by Member States to safeguard their essential State functions, in particular those concerning national...
Amendment 36

Proposal for a regulation
Article 7 – paragraph 6

Text proposed by the Commission

6. The Agency shall organise annual cybersecurity exercises at Union level, and support Member States and EU institutions, agencies and bodies in organising exercises following their request(s). 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. The Agency shall also contribute to and help organise, where appropriate, sectoral cybersecurity exercises together with relevant ISACs and permit ISACs to participate also to Union level cybersecurity exercises.

Amendment

6. The Agency shall organise regular, at least annual cybersecurity exercises at Union level, and support Member States and EU institutions, agencies and bodies in organising exercises following their request(s). 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. The Agency shall also contribute to and help organise, where appropriate, sectoral cybersecurity exercises together with relevant ISACs and permit ISACs to participate also to Union level cybersecurity exercises.

Amendment 37

Proposal for a regulation
Article 7 – paragraph 8 – point c

Text proposed by the Commission

(c) supporting the technical handling of an incident or crisis, including facilitating the sharing of technical solutions between Member States;

Amendment

(c) supporting the technical handling of an incident or crisis, including facilitating the voluntary sharing of technical solutions between Member States;

Or. en
Justification

Establish consistency with limitation added to Art. 7(4)(b)

Amendment 38

Proposal for a regulation
Article 7 – paragraph 8 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Agency shall conduct, upon request, regular independent IT security audits of critical cross-border infrastructures with the objective of identifying possible risks and with a view to identifying recommendations to strengthen their resilience.</td>
<td>Or. en</td>
</tr>
</tbody>
</table>

Amendment 39

Proposal for a regulation
Article 8 – paragraph 1 – point a – point -1 (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>continuously identifying standards, technical specifications and ICT technical specifications</td>
<td>Or. en</td>
</tr>
</tbody>
</table>

Justification

Secure that this should be an ongoing process

Amendment 40

Proposal for a regulation
Article 8 – paragraph 1 – point a – point 1
Text proposed by the Commission

(1) preparing candidate European cybersecurity certification schemes for ICT products and services in accordance with Article 44 of this Regulation;

Amendment

(1) in cooperation with industry stakeholders and standardisation organisations in a formal, standardised and transparent process, preparing candidate European cybersecurity certification schemes for ICT products, processes and services in accordance with Article 44 of this Regulation;

Or. en

Justification

It is important to better include stakeholders in the process of developing cybersecurity certification schemes

Amendment 41

Proposal for a regulation
Article 8 – paragraph 1 – point b

Text proposed by the Commission

(b) facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products and services, as well as draw up, in collaboration with Member States, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148;

Amendment

(b) facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products and services, as well as draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148;

Or. en
Amendment 42

Proposal for a regulation
Article 9 – paragraph 1 – point c

Text proposed by the Commission
(c) provide, in cooperation with experts from Member States authorities, advice, guidance and best practices for the security of network and information systems, in particular for the security of the internet infrastructure and those infrastructures supporting the sectors listed in Annex II of Directive (EU) 2016/1148;

Amendment
(c) provide, in cooperation with experts from Member States authorities and relevant industry stakeholders, advice, guidance and best practices for the security of network and information systems, in particular for the security of the internet infrastructure and those infrastructures supporting the sectors listed in Annex II of Directive (EU) 2016/1148;

Or. en

Justification
Secure a better involvement of industry

Amendment 43

Proposal for a regulation
Article 9 – paragraph 1 – point e

Text proposed by the Commission
(e) raise awareness of the public about cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens and organisations;

Amendment
(e) continuously increase and raise awareness of the public about cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens and organisations;

Or. en

Amendment 44

Proposal for a regulation
Article 9 – paragraph 1 – point g

Text proposed by the Commission
(g) organise, in cooperation with the

Amendment
(g) organise, in cooperation with the
Member States and Union institutions, bodies, offices and agencies regular outreach campaigns to increase cybersecurity and its visibility in the Union.

Member States and Union institutions, bodies, offices and agencies regular communication campaigns to force a broad public debate.

Or. en

Justification

This relates to ENISA’s objective to raise awareness of citizens and businesses (Art. 4(7)): especially the consumers as ‘weakest’ target need to take a different approach to cybersecurity

Amendment 45

Proposal for a regulation
Article 11 – paragraph 1 – point c a (new)

Text proposed by the Commission

Amendment

(c a) providing advice and support to the Commission, in collaboration with the European Cybersecurity Certification Group established under Article 53, on matters concerning agreements for mutual recognition of cybersecurity certificates with third countries.

Or. en

Amendment 46

Proposal for a regulation
Article 20 – paragraph 1

Text proposed by the Commission

Amendment

1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders’ Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups,

1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders’ Group composed of recognised security experts representing the relevant stakeholders, such as the ICT industry, operators of essential services according to the NIS Directive, providers of electronic communications
academic experts in the cybersecurity, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities. networks or services available to the public, SMEs, consumer groups, academic experts in the cybersecurity, European Standards Organisations (ESOs) and conformity assessment bodies and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities.

Justification

It is essential that ENISA strongly involves the relevant EU industry representatives and operators by not overcharging the PSG which should keep its current role as an advisory body.

Amendment 47

Proposal for a regulation
Article 20 a (new)

Text proposed by the Commission

Amendment

Article 20 a

Ad-hoc Consultation platforms

The Management Board, acting on a proposal by the Executive Director, shall set up dedicated ad-hoc consultation platforms which shall, on a case-by-case basis, provide ENISA with further assistance and advice when preparing a certification scheme in accordance with to Title III of this Regulation. This platform shall be open for participation and shall accompany the certification process in close cooperation with the Group established under Article 53. It shall give formal approval of any candidate certification scheme prepared by the Agency before the scheme is transmitted to the European Commission for approval. It shall be dissolved once the certification scheme is adopted. It shall be
composed of representatives of the Permanent Stakeholders’ Group and any other relevant stakeholders, including Union industry representatives with specific expertise in the field of a given candidate scheme.

Or. en

Justification

The creation of a flexible sub-group for each certification process allows a good industry representation, especially of SMEs.

Amendment 48

Proposal for a regulation
Article 21 a (new)

Text proposed by the Commission

Amendment

Article 21 a

Requests to the Agency

1. Requests for advice and assistance on matters falling within the Agency’s objectives and tasks shall be addressed to the Executive Director and accompanied by background information explaining the issue to be addressed. The Executive Director shall inform the Management Board and Executive Board of the requests received, the potential resource implications, and, in due course, of the follow-up to the requests. If the Agency refuses a request, it shall give a justification.

2. The requests referred to in paragraph 1 may be made by:

(a) the European Parliament;
(b) the Council;
(c) the Commission;
(d) any competent body appointed by a Member State, such as a national regulatory authority as defined in Article
2 of Directive 2002/21/EC\textsuperscript{1a}.

3. The practical arrangements for applying paragraphs 1 and 2 regarding in particular to the submission and prioritisation of, follow-up to and information to the Management and Executive Board on the requests to the Agency, shall be laid down by the Management Board in the Agency’s internal rules of operation.


Justification

ENISA receives between 20 and 30 requests for advice and assistance per year. The procedure for these requests is formalised in Art. 14 of Regulation 526/2013 on ENISA and needs to be included in this Regulation as part of the operation of the agency.

Amendment 49

Proposal for a regulation
Article 43 – paragraph 1

\textit{Text proposed by the Commission}

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.

\textit{Amendment}

A European cybersecurity certification scheme shall attest that the ICT products, processes 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 and services throughout their life cycle.
Amendment 50

Proposal for a regulation
Article 44 – paragraph -1 (new)

Text proposed by the Commission

-1. The Commission shall adopt a multiannual Union work programme for European cybersecurity certification schemes, which shall identify common actions to be undertaken at Union level and strategic priorities. The work programme shall in particular include a priority list of identified ICT products, processes and services suitable for being subject to a European cybersecurity certification scheme as well as an analysis as to whether there is an equivalent level of quality, know-how and expertise among the conformity assessment bodies and the national certification supervisory authorities and, if necessary, a proposal of measures how this can be achieved. Prior to adopting the work programme, the Commission shall consult ENISA and have the utmost regard of its opinion.

Justification

The purpose of this work programme is to add transparency and accountability into the process of preparing European cybersecurity certification schemes.

Amendment 51

Proposal for a regulation
Article 44 – paragraph 1

Text proposed by the Commission

1. Following a request from the Commission, ENISA shall prepare a

Amendment

1. The preparation of a candidate European cybersecurity certification
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.**

Scheme may be proposed to the Commission or to the Group by Member States or the Permanent Stakeholders’ Group. 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.

Or. en

**Justification**

For the preparation of candidate schemes, Member States and industry play a vital role as it is industry together with Member States where innovation comes from. Their advice needs to be taken duly into account.

**Amendment 52**

**Proposal for a regulation**  
**Article 44 – paragraph 2**

**Text proposed by 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.

**Amendment**

2. When preparing candidate schemes referred to in paragraph 1 (new) of this Article, ENISA shall consult all relevant stakeholders by transparent consultation processes and closely cooperate with the Group, the Permanent Stakeholders’ Group and, if appropriate, ad hoc consultation platforms in accordance with Article 20a new. They 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.

Or. en

**Justification**

A strong Member States’ and industry involvement requires that they can contribute to the development of the scheme.
Amendment 53

Proposal for a regulation
Article 44 – paragraph 3

Text proposed by the Commission

3. **ENISA shall transmit** the candidate European cybersecurity certification scheme prepared in accordance with paragraph 2 of this Article to the Commission.

Amendment

3. **Upon the approval of** the candidate European cybersecurity certification scheme by the Group, **ENISA shall transmit the candidate** scheme prepared in accordance with paragraph 2 of this Article to the Commission. **The Commission shall assess the compliance of the documents drafted by ENISA with its initial request.**

Or. en

Amendment 54

Proposal for a regulation
Article 44 – paragraph 4

Text proposed by 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.

Amendment

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 products, **processes** and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.

Or. en

Amendment 55

Proposal for a regulation
Article 44 – paragraph 5

Text proposed by the Commission

5. **ENISA shall maintain a dedicated**

Amendment

5. **ENISA shall maintain a dedicated**
website providing information on, and publicity of, European cybersecurity certification schemes.

website providing information on, and publicity of, European cybersecurity certification schemes, including withdrawn and expired certificates, certificates and declarations of conformity.

Or. en

Amendment 56
Proposal for a regulation
Article 44 – paragraph 5 – subparagraph 1 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where a European cybersecurity certification scheme satisfies the requirements which it aims to comply with and which are set out in the corresponding Union harmonisation legislation, the Commission shall publish a reference thereof without delay in the Official Journal of the European Union and by any other means in accordance with the conditions laid down in the corresponding act of Union harmonisation legislation.</td>
<td></td>
</tr>
</tbody>
</table>

Or. en

Amendment 57
Proposal for a regulation
Article 44 – paragraph 5 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 a. The Agency shall review the adopted schemes at least every five years taking into account feedback received from relevant stakeholders.</td>
<td></td>
</tr>
</tbody>
</table>

Or. en
Amendment 58
Proposal for a regulation
Article 45 – paragraph 1 (new)

Text proposed by the Commission

-1. A European cybersecurity certification scheme shall be designed to meet the common cyber security objectives of integrity, confidentiality, availability, and privacy. Furthermore, it shall minimise other risks for life, health, the environment and other important legal interests. It shall be proportionate, market-driven and take into account the public interest.

Or. en

Amendment 59
Proposal for a regulation
Article 45 – paragraph 1 – point a

Text proposed by the Commission

(a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure;

Amendment

(a) ensure the confidentiality, integrity, availability and privacy of services, functions and data;

Or. en

Amendment 60
Proposal for a regulation
Article 45 – paragraph 1 – point b

Text proposed by the Commission

(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss

Amendment

(b) ensure that services, functions and data can only be accessed and used by authorised persons and/or authorised
or alteration; systems and programmes;

Amendment 61
Proposal for a regulation
Article 45 – paragraph 1 – point c

Text proposed by the Commission

(c) ensure that authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;

Amendment

(c) ensure that a process is in place to identify and document all dependencies and known vulnerabilities in ICT products, processes and services;

Amendment 62
Proposal for a regulation
Article 45 – paragraph 1 – point d

Text proposed by the Commission

(d) record which data, functions or services have been communicated, at what times and by whom;

Amendment

(d) ensure that ICT products, processes and services do not contain known vulnerabilities;

Amendment 63
Proposal for a regulation
Article 45 – paragraph 1 – point e

Text proposed by the Commission

(e) ensure that it is possible to check which data, services or functions have been accessed or used, at what times and by whom;

Amendment

(e) ensure that a process is in place to deal with newly discovered vulnerabilities in ICT products, processes and services;
Amendment 64

Proposal for a regulation
Article 45 – paragraph 1 – point f

Text proposed by the Commission

(f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;

Amendment

(f) have in place a process for monitoring, detecting and reporting security incidents and for responding to those incidents and preventing a recurrence;

Amendment 65

Proposal for a regulation
Article 45 – paragraph 1 – point g

Text proposed by the Commission

(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.

Amendment

(g) ensure that availability and access to services, functions and data is minimally perturbed or quickly restored in case of an incident;

Amendment 66

Proposal for a regulation
Article 45 – paragraph 1 – point g a (new)

Text proposed by the Commission

(g a) record which data, functions or services have been communicated, at what times and by whom;
Amendment 67

Proposal for a regulation
Article 45 – paragraph 1 – point g b (new)

Text proposed by the Commission

Amendment

(g b) ensure that it is possible to check which data, services or functions have been accessed or used, at what times and by whom;

Or. en

Amendment 68

Proposal for a regulation
Article 45 – paragraph 1 – point g c (new)

Text proposed by the Commission

Amendment

(g c) ensure that ICT products, products and services are developed according to the principle ‘security by design’.

Or. en

Justification

The wording of the security objectives is too prescriptive, it needs to be more flexible and descriptive

Amendment 69

Proposal for a regulation
Article 46 – paragraph 1

Text proposed by the Commission

Amendment

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels:

1. A European cybersecurity certification scheme may specify one or more of the following risk-based assurance
basic, substantial and/or high, for ICT products and services issued under that scheme.

levels according to the context and intended use of the ICT products, processes and service: basic, substantial and/or high.

Amendment 70

Proposal for a regulation
Article 46 – paragraph 2 – point a

Text proposed by the Commission

(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, including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents;

Amendment

(a) The assurance level basic shall correspond to a low risk related to an ICT product, process and service. A low level of risk exists when an attack on the ICT product, process and service does not compromise the availability, authenticity, integrity, confidentiality or other important objectives such as the health of users or third parties, the environment, privacy, other important legal interests or critical infrastructures and its supporting systems or products.

Justification

It is essential to have a minimum description of what are the assurance components of each assurance level.

Amendment 71

Proposal for a regulation
Article 46 – paragraph 2 – point b

Text proposed by the Commission

(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

Amendment

(b) The assurance level substantial shall correspond to a higher risk related to an ICT product, process and service. A higher level of risk exists when an attack on the ICT product, process and service
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;

compromises the availability, authenticity, integrity, confidentiality or other important objectives such as the health of users or third parties, the environment, privacy, other important legal interests or critical infrastructures and its supporting systems or products.

Or. en

Justification

It is essential to have a minimum description of what are the assurance components of each assurance level.

Amendment 72

Proposal for a regulation
Article 46 – paragraph 2 – point c

Text proposed by the Commission

(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.

Amendment

(c) The assurance level high shall correspond to a high risk related to an ICT product, process and service. A high level of risk exists when an attack on the ICT product, process and service compromises the availability, authenticity, integrity, confidentiality or other important objectives and reasonably endangers the national sovereignty or public security of states.

Or. en

Justification

It is essential to have a minimum description of what are the assurance components of each assurance level.
Amendment 73
Proposal for a regulation
Article 46 a (new)

Text proposed by the Commission

Amendment

Article 46 a

Evaluation of assurance levels of European cybersecurity certification schemes

1. For the assurance level basic, it shall be possible to perform a conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, processes and services as laid down in Article 4 and Annex II of Decision No 768/2008/EC.

2. For the assurance levels substantial and high, the evaluation shall be guided at least by the verification of the conformity of security functionalities of the product, process or service to its technical documentation;

Or. en

Justification

To allow self-certification (called: self-assessment) only at the lowest level will align it to the New Legislative Framework and will allow a cost-effective and easier way of certification of products, processes and services with an intended use for the “mass” market.

Amendment 74
Proposal for a regulation
Article 47 – paragraph 1 – point a

Text proposed by the Commission

(a) subject-matter and scope of the certification, including the type or categories of ICT products and services covered;

Amendment

(a) subject-matter and scope of the certification, including the type or categories of ICT products, processes and services covered as well as a justification of how the certification scheme meets the
needs of the expected target group;

Or. en

Amendment 75

Proposal for a regulation
Article 47 – paragraph 1 – point a a (new)

Text proposed by the Commission

Amendment

(a a) Cybersecurity requirements as stated in the national cybersecurity certifications that it shall replace, or as stated in the legislation and policies to which it shall give support.

Or. en

Justification

To facilitate the transition - the subject matter and scope of the European cybersecurity certification scheme should be linked to the act it replaces or supports, depending on its intention to eliminate barriers to trade or to support legislation and policies.

Amendment 76

Proposal for a regulation
Article 47 – paragraph 1 – point b

Text proposed by the Commission

Amendment

(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;

(b) detailed specification of the cybersecurity requirements against which the specific ICT products, processes and services are evaluated, for example by reference to Union or international standards or technical specifications;

Or. en
Amendment 77

Proposal for a regulation
Article 47 – paragraph 1 – point d a (new)

Text proposed by the Commission

Amendment

(d a) Types of conformity assessment, evaluation criteria and methods as laid down in Article 4 and Annex II of Decision 768/2008/EC, in order to ensure that the specific objectives referred to in Article 45 of this Regulation are met;

Or. en

Justification

This introduces and establishes a link to the New Legislative Framework

Amendment 78

Proposal for a regulation
Article 47 – paragraph 1 – point m a (new)

Text proposed by the Commission

Amendment

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

Or. en

Justification

This aims to achieve harmonisation across the EU.

Amendment 79

Proposal for a regulation
Article 47 – paragraph 1 – point m b (new)

Text proposed by the Commission

Amendment

(m b) the maximum period of validity of the certificate.
Amendment 80
Proposal for a regulation
Article 47 a (new)

Text proposed by the Commission

Amendment

Article 47 a

Product declaration

1. The manufacturer or provider of ICT products, processes and services shall issue a product declaration which shall provide, inter alia, the following relevant information in respect of the certification of this product, process and service:

   - that the requirements set out in the scheme have been satisfied;
   - the interoperability of the product, process and service;
   - that the product, process and service allow for updates and the period during which such updates shall be provided.

By issuing such a declaration, the manufacturer or provider of ICT products, processes and services shall assume responsibility for the compliance of the ICT product or service with the requirements set out in the scheme.

2. The manufacturer or provider of ICT products and services shall keep, for a period of 10 years, the product declaration and the relevant technical documentation relating to the conformity of the ICT products or services with a scheme at the disposal of the national certification supervisory authority referred to in Article 50(1). A copy of the declaration shall be submitted to the national certification supervisory authority and to ENISA.
Justification

*It is in the interest of consumers and industry to know about the specifications of the ICT product, process and service. For this reason, Art. 47 provides for an obligation for manufacturers or providers to issue a product declaration with relevant information. The consumer will then be able to decide on an informed basis.*

**Amendment 81**

**Proposal for a regulation**

**Article 48 – paragraph 2**

**Text proposed by the Commission**

2. The certification shall be voluntary, unless otherwise specified in Union law.

**Amendment**

2. The certification *for the assurance level high shall be mandatory. For the assurance levels basic and substantial it shall be voluntary, unless otherwise specified in Union law.*

*Or. en*

**Justification**

*Highest risk ICT products, processes and services should be subject to mandatory assessment to enhance trust.*

**Amendment 82**

**Proposal for a regulation**

**Article 48 – paragraph 3**

**Text proposed by the Commission**

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.

**Amendment**

3. A European cybersecurity certificate pursuant to this Article shall be issued either by self-assessment or 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.

*Or. en*
Amendment 83

Proposal for a regulation
Article 48 – paragraph 6

Text proposed by the Commission

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

Amendment

6. Certificates shall be issued for a maximum period determined by the rules of the scheme and taking into account a reasonable life-cycle and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.

Or. en

Justification

This ensures flexibility to adjust the validity period to the intended use.

Amendment 84

Proposal for a regulation
Article 48 a (new)

Text proposed by the Commission

Article 48 a

Formal objections to European cybersecurity certification schemes

1. When a Member State considers that a European cybersecurity certification scheme does not entirely satisfy the requirements which it aims to comply with and which are set out in the relevant Union harmonisation legislation, it shall inform the Commission and shall provide a detailed explanation. The Commission shall, after consulting the committee set up in accordance with the relevant Union harmonisation legislation, if applicable, or after other forms of consultation of sectoral experts, decide:
(a) to publish, not to publish or to publish with restriction the references to the European cybersecurity scheme concerned in the Official Journal of the European Union;

(b) to maintain, to maintain with restriction or to withdraw the references to the European cybersecurity scheme concerned in or from the Official Journal of the European Union.

2. The Commission shall publish information on its website on the European cybersecurity schemes that have been subject to the decision referred to in paragraph 1 of this Article.

3. The Commission shall inform ENISA of the decision referred to in paragraph 1 of this Article and, if necessary, request the revision of the European cybersecurity scheme concerned.

4. The decision referred to in point (a) of paragraph 1 of this Article shall be adopted in accordance with the advisory procedure referred to in Article 55(2).

5. The decision referred to in point (b) of paragraph 1 of this Article shall be adopted in accordance with the examination procedure referred to in Article 55(2a new).

Amendment 85

Proposal for a regulation
Article 49 – paragraph 3 a (new)

Text proposed by the Commission

3 a. Member States shall communicate to the Commission all requests to draw up national cybersecurity certification schemes and shall state the grounds for
their enactment.

Amendment 86
Proposal for a regulation
Article 49 – paragraph 3 b (new)

*Text proposed by the Commission*

3 b. Upon request, Member States shall send at least in electronic form any draft national cybersecurity certification scheme to other Member States, ENISA or the Commission.

Amendment

Amendment 87
Proposal for a regulation
Article 49 – paragraph 3 c (new)

*Text proposed by the Commission*

3 c. Within three months, each Member State shall reply to, and take due account of, any comments received from any other Member State, ENISA or the Commission with respect to any draft referred to in paragraph 3b of this Article.

Amendment

Amendment 88
Proposal for a regulation
Article 49 – paragraph 3 d (new)

*Text proposed by the Commission*

3 d. When a Member State receives
comments that the draft national cybersecurity certification scheme would have a negative impact on the internal market, it shall consult ENISA and the Commission before adopting it.

Or. en

Justification

The adding of a notification system aims to prevent creating barriers in the internal market before they materialize and is common practice in standards and technical regulation.

Amendment 89

Proposal for a regulation
Article 50 – paragraph 6 – point b a (new)

Text proposed by the Commission  Amendment

(b a)  carry out audits to ensure that equivalent standards apply in the Union and shall report on the results to ENISA and to the Group;

Or. en

Justification

This helps to ensure that a uniform level of service and quality is applied across the EU and helps to prevent the possibility of “certification shopping”

Amendment 90

Proposal for a regulation
Article 51 – paragraph 2 a (new)

Text proposed by the Commission  Amendment

2 a. Audits shall be carried out to ensure that equivalent standards apply in the Union, the results of which shall be reported to ENISA and to the Group.

Or. en
Amendment 91

Proposal for a regulation
Article 53 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. The Group shall be composed of national certification supervisory authorities from all Member States. The authorities shall be represented by the heads or by other high level representatives of national certification supervisory authorities.

Or. en

Justification

This will make the work of the group more open and transparent.

Amendment 92

Proposal for a regulation
Article 55 – paragraph 2 a (new)

Text proposed by the Commission

2 a. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Amendment

Or. en
EXPLANATORY STATEMENT

It is a fact that the global digital revolution takes hold and proliferates into our economies, societies and governments – all our data is vulnerable. Consumers, industries, institutions and democracies at local, national, European and global level have been victims of cyberattacks, cyber espionage and cyber sabotage and we all are aware that this will increase significantly in the next years.

Billions of devices are being connected to the internet and are interacting on a new level and scale. These devices and related services can improve citizens’ lives and our economies. However, people and organisations will only fully be or become part of the digital world if they have trust in the digital technologies. Trust requires that IoT devices, processes and services are safe and secure.

In order to achieve these objectives, the Commission proposed the ‘Cybersecurity Act’. This Regulation is an important part and tool of the new European Union’s cybersecurity strategy which aims to provide Europe with a long-term vision of cybersecurity and to secure confidence in the digital technologies. It has to be seen in the context of the legislation already in place: The EU has already created a European Agency for Network and Information Security (ENISA) and adopted a network and information security directive (NIS-Directive) which is currently transposed by the Member States.

The ‘Cybersecurity Act’ consists of two parts: In the first part, ENISA’s role and mandate is specified with the aim to strengthen the Agency. In the second part, a European cyber certification scheme is introduced in the form of a voluntary framework to improve the security of connected devices and digital products and services.

In general, the Rapporteur welcomes the Commission’s proposal on the European Cybersecurity Act as it is crucial to minimize risks and threats to information security and network systems and to enable the consumers to have trust and confidence in IT solutions, in particular with regard to the internet of things. The Rapporteur strongly believes that Europe can become a leading player in cybersecurity. Europe has a strong industrial base, and, thus, working on improving cybersecurity with regard to consumer goods, industrial applications and critical infrastructure is in the interest of both, consumers as well as industry.

The Commission’s proposal should be amended, with respect to both, the part on ENISA and the part on certification:

As regards ENISA, the Rapporteur believes that it is crucial to set the right framework if we want a strong and well-functioning Agency. The Rapporteur welcomes a strengthened role for ENISA, comprising its then permanent mandate and an increase of its budget and staff but also a realistic approach is needed, considering the still small number of experts employed by ENISA compared to the size of staff in some national certification supervisory authorities. ENISA’s task should continue to be that of arranging for operational cooperation, by considering expertise gained under the NIS-Directive, to continue supporting capacity building in Member states and to be a source of information. Further, ENISA needs to play a strong role in establishing European cyber security schemes together with the Member States and relevant stakeholders.
As regards the certification, the Rapporteur is in favour of a clearer scope of application of the proposal. Firstly, not only products and services should be covered by this Regulation, but the whole life-cycle. Thus, processes have also to be included in the scope of application. On the other hand, areas of competences from the Member States should be clearly excluded, namely where public security, defence, national security and the area of criminal law are concerned.

As regards the European Cyber Certification Scheme, the Rapporteur proposes to specify in more detail a risk-based approach and not a "one-size fits all" certification scheme. Further, the Rapporteur is in favour of a voluntary system - but only for the basic and substantial assurance levels. For products, processes or services falling under the highest assurance level, a mandatory scheme is preferable according to the Rapporteur. As regards the evaluation of digital technologies falling under the basic assurance level, the Rapporteur further suggests a link to the new legislative framework approach. This will allow self-assessment, a cheaper and less burdensome system which proved to work well in specific different areas.

The rapporteur believes that the manufacturer or provider of ICT products, processes and services should be obliged to issue a mandatory product declaration with structured information concerning the certification, indicating for example the availability of updates or the interoperability of the certified products, process or service. This would provide the consumer with useful information when choosing a device. The Rapporteur prefers such product declaration in comparison to a label or mark which may be misleading for consumers.

The Rapporteur strongly believes that the governance structure as proposed by the Commission needs to be improved to be more transparent for all stakeholders involved. The Rapporteur therefore suggests the adoption of a multiannual Union work programme which shall identify common actions to be undertaken at Union level and which shall indicate the areas where European certification schemes should be established with priority and the level of equivalence of know-how and expertise of assessment and supervisory bodies in the Member States. A reinforced governance also means a stronger Member States’ and industry participation in the certification process: The role of the Member States can be strengthened when the ‘Group’, established under Article 53 of the proposal and composed of national certification supervisory authorities, is to be put on equal footing with the Commission in the preparation process of a certification scheme. The Group will also have to approve a European candidate scheme. Thirdly, also the industry participation in the certification process should be strengthened. This can be achieved by clarifying the composition of the Permanent Stakeholder Group and by establishing ad-hoc-advisory groups by ENISA in order to gain further expertise and know-how by industry and other relevant stakeholders within certification processes. The Rapporteur believes that all these measures will help SMEs to be much more present in the process.

Finally, a European certification system needs a stronger involvement of European standardisation organisations such as CEN and CENELEC when developing new schemes. This would allow that existing and globally accepted international standards prevail.