European Parliament
2014-2019

Committee on the Internal Market and Consumer Protection

2017/0225(COD)

1.2.2018

DRAFT OPINION

of the Committee on the Internal Market and Consumer Protection

for the Committee on Industry, Research and Energy

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))

Rapporteur: (*) Nicola Danti

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

PA_Legam

SHORT JUSTIFICATION

In the digital era, Cybersecurity is an essential element for the economic competitiveness and security of the European Union, and for the integrity of our free and democratic societies and the processes that underpin them. Guaranteeing a high level of cyber resilience across the EU is of paramount importance for achieving consumer trust in the Digital Single Market and for the further development of a more innovative and competitive Europe.

Without a doubt, cyber threats and global cyber-attacks - such as "Wannacry" and "Meltdown" - are issues of increasing importance in our more and more digitalised society. According to a Eurobarometer survey published in July 2017, 87% of respondents regard cyber-crime "as an important challenge to the EU's internal security" and a majority of those are "concerned about being victims of various forms of cybercrime". Moreover, since the beginning of 2016, more than 4,000 ransom-ware attacks have occurred worldwide every day, with a 300% increase since 2015, affecting 80% of the EU companies. These facts and findings clearly show a need for the EU to be more resilient and effective in combatting cyber-attacks and to increase its capabilities to better protect Europe's citizens, businesses and public institutions.

One year after the entry into force of the NIS Directive, the European Commission, in the broader framework of the EU cybersecurity strategy, presented a Regulation that aims at further increasing EU cyber resilience, deterrence and defence. On 13 September 2017, the Commission presented the "Cybersecurity act", based on two pillars:
1) a permanent and stronger mandate for the European Agency for Network and Information Security (ENISA) to assist Member States in effectively preventing and responding to cyber-attacks and 2) the creation of a EU cybersecurity certification framework to ensure ICT products and services are cyber secure.

In general, the Rapporteur welcomes the approach proposed by the European Commission and especially favours the introduction of EU-wide cybersecurity certification schemes, which aim at increasing the safety of ICT products and services and at avoiding the costly fragmentation of the Single Market in this crucial field. Even though initially it should remain a voluntary tool, the Rapporteur hopes that an EU framework for cybersecurity certification and related procedures will become a necessary tool to bolster the trust of our citizens and users and to increase the security in products and services that circulate in the Single Market.

Indeed, he is also convinced that a number of points of the proposal should be clarified and improved:

- First of all, **increasing the involvement of relevant stakeholders in the different phases of the governance-system for the preparation of candidate certification schemes by ENISA**: in the Rapporteur's view, it is essential to formally involve the most relevant stakeholders such as ICT industries, consumer organisations, SMEs, EU standards organisations bodies and EU sectoral agencies etc., and give them the possibility to propose new candidate schemes, advise ENISA with their expertise, or cooperate with ENISA in the preparation of a candidate scheme.
- Secondly, there is a need to strengthen the coordinating role of the European Cybersecurity Certification Group (composed by national authorities, supported by the Commission and ENISA) with the additional tasks to provide strategic guidance and to **establish a work programme in respect of common actions to be undertaken at**

Union level in the field of certification as well as to establish and **periodically update a priority list of ICT products and services** for which it considers a European cybersecurity certification scheme to be needed.

- The Rapporteur strongly believes that we should avoid the practice of EU certification "shopping", as has already happened in other sectors. The **monitoring and surveillance provisions of ENISA and the national certification supervisory authorities should be strongly reinforced,** in order to guarantee that a European certificate issued in a Member state will have the same standards and requirements as one issued in another Member state. Therefore he proposes:

  1) to strengthen the surveillance powers of ENISA: together with the Certification Group, ENISA should carry out assessments of the procedures put in place by the authorities responsible for the issuance of EU certificates;
  2) that the national certification supervisory authorities should carry out periodic assessments (at least every two years) on the EU certificates issued by conformity assessment bodies;
  3) to introduce common binding criteria to be defined by the Group for setting out the scale, scope and frequency with which national certification supervisory authorities should carry out assessments referred to under point 2.
- The Rapporteur believes that a mandatory **EU Trust Label** should be introduced for certified ICT products and services, which are intended for end users. This label could help raise awareness of cybersecurity and give companies with good cybersecurity credentials a competitive edge.
- The Rapporteur agrees with the uniform and harmonised approach taken by the Commission, but he is convinced that it should be more flexible and adaptable to the specific characteristics and vulnerabilities of each product or service - no "one size-fits-all" principle. Therefore, the Rapporteur believes that **assurance levels** should be re-named and should be used also taking account of the intended use of ICT products and services. Similarly, the duration of **validity of the certificate** should be defined on a scheme-by-scheme basis.
- Each certification scheme should be designed in such a way as to stimulate and encourage all actors involved in the sector concerned to develop and adopt security standards, technical norms and **security-by-design and privacy-by-design principles**, at all stages of the product or service lifecycle.

AMENDMENTS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, ***the*** trust in the digital single market should be further improved by offering transparent information on the level of security of ICT products and services. This can be facilitated by EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors.	(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, ***given that cyber incidents undermine*** trust ***in digital service providers and*** in the digital single market ***itself, especially among consumers, trust*** should be further improved by offering transparent information on the level of security of ICT products and services. This can be facilitated by EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors. ***Alongside Union-wide certification, there are a range of voluntary measures that the private sector itself should take to bolster trust in the security of ICT products and***

services, in particular in view of the growing availability of IoT devices. For example, more effective use should be made of encryption and other technologies such as blockchain, in order to improve the security of end-users' data and communications and the overall security of network and information systems in the Union.

Or. en

Amendment 2

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) The Union has already taken important steps to ensure cybersecurity and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to cybersecurity threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). The NIS Directive put in place requirements concerning national capabilities in the area of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for economy and society such as energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces). A key role was	(7) The Union has already taken important steps to ensure cybersecurity and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to cybersecurity threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive***, the success of which will depend heavily on effective implementation by Member States,*** put in place requirements concerning national capabilities in the area of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for economy and society such as energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search

attributed to ENISA in supporting implementation of this Directive. In addition, effective fight against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity.

engines, cloud computing services and online marketplaces). A key role was attributed to ENISA in supporting implementation of this Directive. In addition, effective fight against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity.

Or. en

Amendment 3

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) The Agency should contribute towards raising the awareness of the public about risks related to cybersecurity and provide guidance on good practices for individual users aimed at citizens and organisations. The Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing publicly available information regarding significant incidents, and by compiling reports with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting basic authentication ***and*** data protection ***advice***. The Agency should play a central role in accelerating end-user awareness on	(28) The Agency should contribute towards raising the awareness of the public about risks related to cybersecurity and provide guidance on good practices for individual users aimed at citizens and organisations. The Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing publicly available information regarding significant incidents, and by compiling reports with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting ***advice on*** basic authentication***,*** data protection***, encryption and other security- and privacy-enhancing technologies and***

security of devices.

anonymisation tools. The Agency should play a central role in accelerating end-user awareness on security of devices.

Or. en

Amendment 4

Proposal for a regulation
Recital 36 a (new)

Text proposed by the Commission	*Amendment*
	(36 a) Standards are a voluntary, market-driven tool providing technical requirements and guidance and resulting from an open, transparent and inclusive process. The use of standards facilitates compliance of goods and services with Union law and supports European policies in line with Regulation (EU) No 1025/2012 on European standardisation. The Agency should regularly consult and work in cooperation with the European standardisation organisations, in particular when preparing European cybersecurity certification schemes.

Or. en

Amendment 5

Proposal for a regulation
Recital 44

Text proposed by the Commission	*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,	(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.

should focus on issues relevant to stakeholders and bring them to the attention of the Agency. ***In order to ensure proper involvement of stakeholders in the cybersecurity certification framework, the Permanent Stakeholders' Group should also give advice on which ICT products and services to cover in future European cybersecurity certification schemes, and should make proposals to the Commission to request the Agency to prepare candidate schemes on such ICT products and services.*** 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.

Or. en

Amendment 6

Proposal for a regulation
Recital 52

Text proposed by the Commission	*Amendment*
(52) In view of the above, it is necessary to establish a European cybersecurity certification framework laying down the main horizontal requirements for European cybersecurity certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping national cybersecurity certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should be non-discriminatory and	(52) In view of the above, it is necessary to establish a European cybersecurity certification framework laying down the main horizontal requirements for European cybersecurity certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States***. In so doing, it is essential to build on existing national and international schemes, as well as on mutual recognition systems, in particular SOG-IS, and to make possible a smooth transition from existing schemes under such systems to schemes under the new European framework***. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have

based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.

been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping national cybersecurity certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should be non-discriminatory and based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.

Or. en

Amendment 7

Proposal for a regulation
Recital 55

Text proposed by the Commission	*Amendment*
(55) The purpose of European cybersecurity certification schemes should be to ensure that ICT products and services certified under such a scheme comply with specified requirements. Such requirements concern the ability to resist, at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products and services. ICT products and services and related cybersecurity needs are so diverse that it is very difficult to come up with general cybersecurity requirements valid across the board. It is, therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, complemented by a set of specific cybersecurity objectives that need to be taken into account when	(55) The purpose of European cybersecurity certification schemes should be to ensure that ICT products and services certified under such a scheme comply with specified requirements. Such requirements concern the ability to resist, at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products and services. ICT products and services and related cybersecurity needs are so diverse that it is very difficult to come up with general cybersecurity requirements valid across the board. It is, therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, complemented by a set of specific cybersecurity objectives that need to be taken into account when

designing European cybersecurity certification schemes. The modalities with which such objectives will be achieved in specific ICT products and services should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications.

designing European cybersecurity certification schemes. The modalities with which such objectives will be achieved in specific ICT products and services should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications. ***It is of paramount importance that each European cybersecurity certification scheme be designed in such a way as to stimulate and encourage all actors involved in the sector concerned to develop and adopt security standards, technical norms and security-by-design and privacy-by-design principles, at all stages of the product or service lifecycle.***

Or. en

Amendment 8

Proposal for a regulation
Recital 56

Text proposed by the Commission	*Amendment*
(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 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	(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 adopt the European cybersecurity certification scheme by means of implementing acts***. In order to underpin trust and predictability in, and raise public awareness of, the cybersecurity certification framework, ENISA should maintain a dedicated website with an easy-to-use online tool listing information on adopted schemes, candidate schemes, and schemes requested by the Commission***. Taking account of the general purpose and security objectives identified in this Regulation, European

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***.

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 ***associated with the operation and use of an ICT product, process or service***, as well as the intended level of assurance: ***secure, substantially secure, highly secure, or any combination thereof***. ***One valuable element that should be included in certification schemes is the use of marks or labels to indicate a certain level of cybersecurity assurance, especially for ICT products and services intended for end-users. Such marks or labels would help to raise awareness of cybersecurity issues among consumers and empower them to make informed choices by providing them with clear and understandable information about ICT products and services, including in relation to software updates, and give companies with good cybersecurity credentials a competitive edge. Such a label could be in the form of a digital logo or QR code, and would provide cybersecurity ratings or indicate the risks associated with the operation and use of an IoT device, on the basis of the requirements set out in the NIS Directive. In order to promote the use of marks or labels, the Commission should propose the introduction of a Union Trust label for ICT products and services intended for end-users.***

Or. en

Amendment 9

Proposal for a regulation
Recital 59

Text proposed by the Commission	*Amendment*
(59) It is necessary to require all Member States to designate one cybersecurity certification supervisory authority to supervise compliance of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory with the requirements of this Regulation and of the relevant cybersecurity certification schemes. National certification supervisory authorities should 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. Moreover, they should cooperate with other national certification supervisory authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.	(59) It is necessary to require all Member States to designate one cybersecurity certification supervisory authority to supervise compliance of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory with the requirements of this Regulation and of the relevant cybersecurity certification schemes. National certification supervisory authorities should 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. Moreover, they should cooperate with other national certification supervisory authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes. ***Effective cooperation among the national certification supervisory authorities is essential for the proper implementation of European cybersecurity certification schemes and of technical issues concerning the cybersecurity of ICT products and services. The Commission should facilitate that exchange of information by making available a general electronic information support system, for example the Information and Communication System on Market Surveillance (ICSMS) and the rapid alert system for dangerous non-food products***

	(RAPEX) already used by market surveillance authorities pursuant to Regulation (EC) No 765/2008.

Or. en

Amendment 10

Proposal for a regulation
Recital 63

Text proposed by the Commission	*Amendment*
(63) In order to specify further the criteria for the accreditation of conformity assessment bodies, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. The Commission should carry out appropriate consultations during its preparatory work, including at expert level. Those consultations should be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	***deleted***

Or. en

Amendment 11

Proposal for a regulation
Recital 65

Text proposed by the Commission	*Amendment*
(65) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT products and services; on modalities of carrying enquiries by the Agency; as well as on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national certification supervisory authorities to the Commission.	(65) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT products and services; on modalities of carrying enquiries by the Agency; as well as on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national certification supervisory authorities to the Commission***, taking into account the proven effectiveness of the electronic notification tool "New Approach Notified and Designated Organisations" (NANDO)***.

Or. en

Amendment 12

Proposal for a regulation
Article 2 – paragraph 1 – point 11

Text proposed by the Commission	*Amendment*
(11) 'ICT product and service' means ***any*** element ***or group of elements*** of network and information systems;	(11) 'ICT product and service' means ***a product, service, process, system, or combination thereof that is an*** element of network and information systems;

Or. en

Amendment 13

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

Text proposed by the Commission	*Amendment*
	(11 a) "national certification supervisory authority" means an authority of a Member State responsible for carrying out

monitoring, enforcement and supervisory tasks in relation to cybersecurity certification on its territory;

Or. en

Justification

It is advisable to include a definition of this entity.

Amendment 14

Proposal for a regulation
Article 3 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. The Agency shall undertake the tasks assigned to it by this Regulation for the purpose of contributing to ***achieving*** a high ***common*** level of cybersecurity within the Union***, to reduce fragmentation in the internal market and improve its functioning***.

Or. en

Amendment 15

Proposal for a regulation
Article 4 – paragraph 5

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

Or. en

Amendment 16

Proposal for a regulation
Article 4 – paragraph 6

Text proposed by the Commission	*Amendment*
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.	6. The Agency shall promote the use of certification ***and standardisation while avoiding the fragmentation caused by lack of coordination between existing certification schemes in the Union. The Agency shall contribute*** 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.

Or. en

Amendment 17

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

Text proposed by the Commission	*Amendment*
	(1 a) carrying out, in cooperation with the European Cybersecurity Certification Group, assessments of the procedures for issuing European cybersecurity certificates put in place by conformity assessment bodies referred to in Article 51, which aim at ensuring the uniform application of this Regulation by conformity assessment bodies when issuing certificates;

Or. en

Amendment 18

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

Text proposed by the Commission	*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, 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;	(b) ***consult the European standardisation organisations on the development of European standards, to ensure the appropriateness of standards used in approved certification schemes and*** 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;

Or. en

Amendment 19

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, academic experts in the cybersecurity, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications	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, ***associations of small and medium-sized enterprises,*** providers of electronic communications networks or services available to the public, consumer groups ***and associations***, academic experts in the ***field of*** cybersecurity***, the European standardisation organisations, as defined***

Code] as well as of law enforcement and data protection supervisory authorities.	***in point (8) of Article 2 of Regulation (EU) No 1025/2012, the relevant sectoral Union agencies and 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.

Or. en

Justification

It is important to ensure that the Permanent Stakeholders' Group is composed of all relevant stakeholders

Amendment 20

Proposal for a regulation
Article 20 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Permanent Stakeholders' Group shall advise the Agency in respect of the performance of its activities. It shall in particular advise the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on all issues related to the work programme.	5. The Permanent Stakeholders' Group shall advise the Agency in respect of the performance of its activities. It shall in particular advise the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on all issues related to the work programme. ***It may also propose that the Commission to request the Agency to prepare candidate European cybersecurity certification schemes in accordance with Article 44.***

Or. en

Justification

This ties in with Article 44(1). Given the expertise available in the broadened composition of the Permanent Stakeholders' Group, it is appropriate that it also has the power to propose certification schemes.

Amendment 21

Proposal for a regulation
Article 44 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	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**,** the European Cybersecurity Certification Group (the 'Group') established under Article 53 ***or the Permanent Stakeholders' Group*** may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.

Or. en

Justification

See justification linked to Article 20(5).

Amendment 22

Proposal for a regulation
Article 44 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult ***the Permanent Stakeholders' Group, in particular the European standardisation organisations, and all other*** 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. ***Where relevant, ENISA may also set up a stakeholder expert group, composed of***

	members of the Permanent Stakeholders' Group and any other relevant stakeholders with specific expertise in the field of a given candidate scheme, in order to provide further assistance and advice.

Or. en

Justification

Since the Permanent Stakeholders' Group exists, it should be named here as having consultation rights. European Standardisation Organisations will play a crucial role in the certification procedure, so ENISA should be obliged to cooperate closely with them. Also, because the range of ICT products and services that might be subject to a scheme is so very broad, setting up expert groups with specific expertise in the field of a given candidate scheme would be a good way of ensuring the scheme is well prepared.

Amendment 23

Proposal for a regulation
Article 44 – paragraph 5

Text proposed by the Commission	*Amendment*
5. ENISA shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes.	5. ENISA shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes***, including information on all candidate schemes that the Commission has requested ENISA to prepare***.

Or. en

Justification

In the interests of transparency and predictability, the website should include information not only on finalised schemes, but also on all schemes that the Commission has requested ENISA to prepare.

Amendment 24

Proposal for a regulation
Article 45 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
A European cybersecurity certification scheme shall be so designed to take into account***, as applicable,*** the following security objectives:	***Each*** European cybersecurity certification scheme shall be so designed to take into account ***at least*** the following security objectives:

Or. en

Amendment 25

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

Text proposed by the Commission	*Amendment*
(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***.***	(g) ensure that ICT products and services are provided with ***up-to-date*** software ***and hardware,*** that does not contain known vulnerabilities, and are provided ***with*** mechanisms for secure software ***and hardware*** updates***, including automatic security updates;***

Or. en

Amendment 26

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

Text proposed by the Commission	*Amendment*
	(g a) ensure that ICT products and services are developed according to the principle of "security by design".

Or. en

Justification

It is of utmost importance that all players in the value chain should ensure their products and services are cybersecure in a dynamic manner from the earliest stage of the engineering process.

Amendment 27

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***: basic, substantial and/or high,*** for ICT products and services issued under that scheme.	1. ***Each*** European cybersecurity certification scheme may specify one or more of the following assurance levels - ***"functionally secure", "substantially secure" and/or "highly secure"*** -for ICT products and services issued under that scheme***, taking into account, inter alia, their intended use***.

Or. en

Justification

The level of assurance of each cybersecurity certification scheme should take into account the use or the destination of the ICT product and service, and not the ICT product and service itself.

Amendment 28

Proposal for a regulation
Article 46 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The assurance levels ***basic, substantial and high*** shall meet the following criteria respectively:	2. The assurance levels ***"functionally secure", "substantially secure" and "highly secure"*** shall meet the following criteria respectively:

Or. en

Amendment 29

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

Text proposed by the Commission	*Amendment*
(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;	(a) assurance level ***"functionally secure"*** shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides ***an adequate*** 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;

Or. en

Amendment 30

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

Text proposed by the Commission	*Amendment*
(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;	(b) assurance level ***"substantially secure"*** 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;

Or. en

Amendment 31

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

Text proposed by the Commission	*Amendment*
(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.	(c) assurance level ***"highly secure"*** 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 ***"substantially secure"***, 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.

Or. en

Amendment 32

Proposal for a regulation
Article 47 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ***A*** European cybersecurity certification scheme shall include the following elements:	1. ***Each*** European cybersecurity certification scheme shall include ***at least*** the following elements:

Or. en

Amendment 33

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

Text proposed by the Commission	*Amendment*
(f) where the scheme provides for marks or labels, the conditions under which	(f) where the scheme provides for marks or labels***, such as an EU Trust label***, the conditions under which such

such marks or labels may be used;	marks or labels may be used***. All schemes covering ICT products or services intended for end-users shall provide for marks or labels***;

Or. en

Justification

An EU trust label should be developed in order to help end-users to make informed choices and raise awareness of cybersecurity issues.

Amendment 34

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

Text proposed by the Commission	*Amendment*
(g) ***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;	(g) the rules for monitoring compliance with the requirements of the certificates, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;

Or. en

Justification

Surveillance should be a central element in every scheme.

Amendment 35

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

Text proposed by the Commission	*Amendment*
(h) conditions for granting, maintaining, continuing, extending and reducing the scope of certification;	(h) conditions for granting, maintaining, continuing***, renewing***, extending and reducing the scope of certification;

Or. en

Amendment 36

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

Text proposed by the Commission	*Amendment*
(l) identification of national cybersecurity certification schemes covering the same type or categories of ICT products and services;	(l) identification of national ***and international*** cybersecurity certification schemes covering the same type or categories of ICT products and services;

Or. en

Amendment 37

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

Text proposed by the Commission	*Amendment*
	(m a) maximum period of validity of certificates, if applicable.

Or. en

Justification

Linked with amendment to Article 48(6).

Amendment 38

Proposal for a regulation
Article 48 – paragraph 4 – introductory part

Text proposed by the Commission	*Amendment*
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	4. By the way of derogation from paragraph 3, in duly justified cases***, such as for national security reasons,*** 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:	public body shall be one of the following:

Or. en

Amendment 39

Proposal for a regulation
Article 48 – paragraph 5

Text proposed by the Commission	*Amendment*
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.	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**,** ***including information on any known security vulnerabilities or risks***.

Or. en

Amendment 40

Proposal for a regulation
Article 48 – paragraph 6

Text proposed by the Commission	*Amendment*
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.	6. Certificates shall be issued for ***the*** period ***defined in each certification scheme*** and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.

Or. en

Justification

Given the vast and varied range of ICT products and service for which schemes might be developed, it seems arbitrary to set a maximum validity period in this Regulation.

Amendment 41

Proposal for a regulation
Article 50 – paragraph 6 – point a

Text proposed by the Commission	*Amendment*
(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;	(a) monitor and enforce the application of the provisions under this Title at national level and ***verify*** 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 ***in accordance with the rules adopted by the European Cybersecurity Certification Group pursuant to point (da) of Article 53(3)***;

Or. en

Justification

The monitoring and surveillance provisions of the national certification supervisory authorities should be strongly reinforced in order to avoid the practice of EU certification "shopping". According to this provision, national certification supervisory authorities have to verify the compliance of a number of certificates issued by conformity assessment bodies to be defined by the Group.

Amendment 42

Proposal for a regulation
Article 50 – paragraph 6 – point b

Text proposed by the Commission	*Amendment*
(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;	(b) monitor**,** supervise ***and, at least every two years, assess*** 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;

Or. en

Justification

The monitoring and surveillance provisions of the national certification supervisory authorities should be strongly reinforced in order to avoid the practice of EU certification "shopping". National certification supervisory authorities have to carry out assessments on the activities of the conformity assessment bodies every two years.

Amendment 43

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

Text proposed by the Commission	*Amendment*
	(b a) report the results of verifications under point (a) and assessments under point (b) to the European Cybersecurity Certification Group and to ENISA;

Or. en

Amendment 44

Proposal for a regulation
Article 50 – paragraph 6 – point d

Text proposed by the Commission	*Amendment*
(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;	(d) cooperate with other national certification supervisory authorities**,** ***national accreditation bodies*** 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;

Or. en

Justification

The cooperation between national certification supervisory authorities and national accreditation bodies is very important, for example the latter will keep the former informed of the list of conformity assessment bodies, including, when applicable, any suspension or withdrawals of accreditation of conformity assessment bodies.

Amendment 45

Proposal for a regulation
Article 50 – paragraph 7 – point e

Text proposed by the Commission	*Amendment*
(e) ***to*** withdraw, in accordance with national law, certificates that are not compliant with this Regulation or a European cybersecurity certification scheme;	(e) withdraw, in accordance with national law, certificates that are not compliant with this Regulation or a European cybersecurity certification scheme ***and inform the national accreditation body accordingly***;

Or. en

Justification

See justification Article 50(6)(d).

Amendment 46

Proposal for a regulation
Article 50 – paragraph 8 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	The Commission shall make available a general electronic information support system for the purpose of that exchange.

Or. en

Justification

Experience shows that information exchange between Member States is often hindered by lack of an appropriate system for that exchange.

Amendment 47

Proposal for a regulation
Article 53 – paragraph 3 – point -a (new)

Text proposed by the Commission	*Amendment*
	(-a) to provide strategic guidance and to establish a work programme in respect of common actions to be undertaken at Union level to ensure the consistent application of this Title;

Or. en

Amendment 48

Proposal for a regulation
Article 53 – paragraph 3 – point -a a (new)

Text proposed by the Commission	*Amendment*
	(-a a) to establish and periodically update a priority list of ICT products and services for which it considers a European cybersecurity certification scheme to be needed;

Or. en

Amendment 49

Proposal for a regulation
Article 53 – paragraph 3 – point d a (new)

Text proposed by the Commission	*Amendment*
	(d a) to adopt binding rules setting out the frequency with which national certification supervisory authorities are to carry out verifications of certificates in accordance with point (a) of Article 50(6), and the criteria, the scale and scope of such verifications, and to adopt common criteria for the format of reporting provided for in point (ba) of Article 50(6);

Or. en

Justification

Linked with the idea developed in Article 50(6)(a).

Amendment 50

Proposal for a regulation
Article 53 – paragraph 3 – point e

Text proposed by the Commission	*Amendment*
(e) to examine the relevant developments in the field of cybersecurity certification and exchange good practices on cybersecurity certification schemes;	(e) to examine the relevant developments in the field of cybersecurity certification and exchange ***information and*** good practices on cybersecurity certification schemes;

Or. en

Amendment 51

Proposal for a regulation
Article 53 – paragraph 3 – point f a (new)

Text proposed by the Commission	*Amendment*
	(f a) to exchange best practices in relation to investigations of conformity assessment bodies and European cybersecurity certificate holders.

Or. en