OPINION

of the Committee on the Internal Market and Consumer Protection

for the Committee on Industry, Research and Energy


Rapporteur: (*) Nicola Danti

(*) Associated committee – Rule 54 of the Rules of Procedure
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 renamed 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 1

Text proposed by the Commission

(1) Network and information systems and telecommunications networks and services play a vital role for society and have become the backbone of economic growth. Information and communications technology underpins the complex systems which support societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and in particular support the functioning of the internal market.

Amendment

(1) Network and information systems and telecommunications networks and services play a vital role for society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and in particular support the functioning of the internal market.

Amendment 2

Proposal for a regulation
Recital 2

Text proposed by the Commission

(2) The use of network and information systems by citizens, businesses and governments across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the Internet of Things (IoT) millions, if not billions, of connected digital devices are expected to be deployed across the EU during the next decade. While an increasing number of devices are connected to the Internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In this context, the limited use of certification leads to insufficient

Amendment

(2) The use of network and information systems by citizens, businesses and governments across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the Internet of Things (IoT) millions, if not billions, of connected digital devices are expected to be deployed across the EU during the next decade. While an increasing number of devices are connected to the Internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In this context, the limited use of certification leads to insufficient
information for organisational and individual users about the cybersecurity features of ICT products and services, undermining trust in digital solutions.

Amendment 3
Proposal for a regulation
Recital 3

Text proposed by the Commission

(3) Increased digitisation and connectivity lead to increased cybersecurity risks, thus making society at large more vulnerable to cyber threats and exacerbating dangers faced by individuals, including vulnerable persons such as children. In order to mitigate this risk to society, all necessary actions need to be taken to improve cybersecurity in the EU to better protect network and information systems, telecommunication networks, digital products, services and devices used by citizens, governments and business – from SMEs to operators of critical infrastructures – from cyber threats.

Amendment

(3) Increased digitisation and connectivity lead to considerably increased cybersecurity risks, thus making society at large more vulnerable to cyber threats and exacerbating dangers faced by individuals, including vulnerable persons such as children. The transformative power of Artificial Intelligence and machine learning will be harnessed by society at large, but also by cyber criminals. In order to mitigate these risks to society, all necessary actions need to be taken to improve security against cyber-attacks in the EU to better protect network and information systems, telecommunication networks, digital products, services and devices used by citizens, governments and business – from SMEs to operators of critical infrastructures – from cyber threats.

Amendment 4
Proposal for a regulation
Recital 4

Text proposed by the Commission

(4) Cyber-attacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyber-attacks are often cross-border, policy responses by
cybersecurity authorities and law enforcement competences are predominantly national. Large-scale cyber incidents could disrupt the provision of essential services across the EU. This requires effective EU level response and crisis management, building upon dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of cybersecurity and resilience in the Union, based on reliable Union data, as well as systematic forecast of future developments, challenges and threats, both at Union and global level, is therefore important for policy makers, industry and users.

Amendment 5
Proposal for a regulation
Recital 5

Text proposed by the Commission

(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

cybersecurity authorities and law enforcement competences are predominantly national. Large-scale cyber incidents could disrupt the provision of essential services across the EU. This requires effective EU level response and crisis management, building upon dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of cybersecurity and resilience in the Union, based on reliable Union data, as well as systematic forecast of future developments, challenges and threats, both at Union and global level, is therefore important for policy makers, industry and users.

Moreover, **given that cyber incidents undermine trust in digital service providers and** in the digital single market
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.

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 standardised EU-wide certification, relying on European or international standards and 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 as well as technologies to prevent successful cyber-attacks 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.

Amendment 6
Proposal for a regulation
Recital 5 a (new)

Text proposed by the Commission

(5a) While certification and other forms of conformity assessment for ICT processes, products and services plays an important role, improving cybersecurity requires a multi-faceted approach spanning people, processes, and technologies. The EU should also continue to strongly emphasise and promote other efforts including cybersecurity education, training, and skills development; raising awareness at corporate executive and board-levels; promoting voluntary cyber threat information sharing; and shifting the EU from a reactive to a proactive approach to responding to threats by emphasising the
prevention of successful cyber-attacks.

Amendment 7

Proposal for a regulation
Recital 7

Text proposed by the Commission

(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 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.

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, 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 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.
Amendment 8
Proposal for a regulation
Recital 11

Text proposed by the Commission

(11) Given the increasing cybersecurity challenges the Union is facing, the financial and human resources allocated to the Agency should be increased to reflect its enhanced role and tasks, and its critical position in the ecosystem of organisations defending the European digital ecosystem.

Amendment

(11) Given the increasing cybersecurity threats and challenges the Union is facing, the financial and human resources allocated to the Agency should be increased to reflect its enhanced role and tasks, and its critical position in the ecosystem of organisations defending the European digital ecosystem.

Amendment 9
Proposal for a regulation
Recital 28

Text proposed by the Commission

(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

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 cyber-hygiene best practices and solutions, meaning simple routine measures that individuals and organisations can take to minimise the risks from cyber threats, such as multi-factor authentication, patching, encryption, and access management. The Agency should do this by collecting and analysing publicly available information regarding significant incidents, and by compiling and publishing reports and guidelines 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

10/64
authentication and data protection advice. The Agency should play a central role in accelerating end-user awareness on security of devices.

campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of measures that can be taken to guard against potential threats in cyberspace, including cybercrimes such as phishing attacks, ransomware attacks, hijacking, botnets, financial and banking fraud, as well as promoting advice on basic multi-factor authentication, encryption, patching, access management principles, data protection, and other security- and privacy-enhancing technologies and anonymisation tools. The Agency should play a central role in accelerating end-user awareness on security of devices and secure use of services, promoting security-by-design at Union level, which is paramount to improving the security of connected devices especially for vulnerable end-users including children, and privacy-by-design. The Agency should encourage all end users to take appropriate steps to prevent and minimise the impact of incidents affecting the security of their networks and information systems. Partnerships should be established with academic institutions that have research initiatives in the relevant areas of cybersecurity.

Amendment 10

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

Amendment

(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.

ENISA should make such warnings public on the website dedicated to providing information on certification schemes. The Agency should draw up guidelines on minimum security requirements for IT devices sold in or exported from the Union. Such guidelines could call for manufacturers to provide a written declaration confirming that a device does not contain hardware, software or firmware components with any known exploitable security vulnerabilities nor any unchangeable or uncrypted password or access code that it is capable of accepting trusted and properly authenticated security updates, that vendors’ response to an affected device includes an adequate hierarchy of remedies and that the vendors inform end-users when security support for a device will end.

Amendment 11
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
Amendment 12

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, academia 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. 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, either on its own initiative or following submission of proposals from relevant stakeholders. 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 efficient and equitable representation of stakeholders in the work of the Agency.

Amendment 13

Proposal for a regulation
Recital 46

Text proposed by the Commission

(46) In order to guarantee the full

Amendment

(46) In order to guarantee the full
autonomy and independence of the Agency and to enable it to perform additional and new tasks, including unforeseen emergency tasks, the Agency should be granted a sufficient and autonomous budget whose revenue comes primarily from a contribution from the Union and contributions from third countries participating in the Agency’s work. The majority of the Agency staff should be directly engaged in the operational implementation of the Agency’s mandate. The host Member State, or any other Member State, should be allowed to make voluntary contributions to the revenue of the Agency. The Union’s budgetary procedure should remain applicable as far as any subsidies chargeable to the general budget of the Union are concerned. Moreover, the Court of Auditors should audit the Agency’s accounts to ensure transparency and accountability.

Amendment 14

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 and practices comprised in a product, process, service, system, or a combination of those (“ICT products and services”) by an independent third party or through a procedure of self-declaration of conformity. Certification cannot guarantee per se that certified ICT products and services are cyber secure and the end user should be made aware of it. It is rather a
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 15
Proposal for a regulation
Recital 48

Text proposed by the Commission
(48) Cybersecurity certification plays an important role in increasing trust and security in ICT products and services. The digital single market, and particularly the data economy and the Internet of Things, can only thrive if there is general public trust that such products and services provide a certain level of cybersecurity assurance. Connected and automated cars, electronic medical devices, industrial automation control systems or smart grids are only some examples of sectors in which certification is already widely used or is likely to be used in the near future. The sectors regulated by the NIS Directive are also sectors in which cybersecurity certification is critical.

Amendment
(48) European cybersecurity certification plays an essential role in increasing trust and security in ICT products and services. The digital single market, and particularly the data economy and the Internet of Things, can only thrive if there is general public trust that such products and services provide a high level of cybersecurity assurance. Connected and automated cars, electronic medical devices, industrial automation control systems or smart grids are only some examples of sectors in which certification is already widely used or is likely to be used in the near future. The sectors regulated by the NIS Directive are also sectors in which cybersecurity certification is critical.

Amendment 16
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

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
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 17

Proposal for a regulation
Recital 52

Text proposed by the Commission

(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 based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the

Amendment

(52) In view of the above, it is necessary to adopt a common approach and 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 been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping
EU’s legitimate objectives in that regard. national cybersecurity certifications and thus reduce costs for undertakings operating in the digital single market. Where a European cybersecurity certification has replaced a national scheme, certificates issued under the European scheme should be accepted as valid in cases where certification under a national scheme was required. The schemes should be guided by security-by-design and the principles referred to in Regulation (EU) 2016/679. They should also 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.

Amendment 18
Proposal for a regulation
Recital 52 a (new)

Text proposed by the Commission

(52a) The European cybersecurity certification framework should be established in a uniform manner in all Member States in order to prevent ‘certification shopping’ based on differences in costs or levels of stringency between Member States.

Amendment 19
Proposal for a regulation
Recital 55

Text proposed by the Commission

(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...
and services certified under 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 processes, products, 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.

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 principles, at all stages of the product or service lifecycle. Where the certification scheme provides for marks or labels, the conditions under which such marks or labels may be used have to be outlined. Such label, which could be in the form of a digital logo or QR code, would indicate the risks associated with the operation and use of ICT products and services and should be clear and easily understandable.
Amendment 20
Proposal for a regulation
Recital 55 a (new)

Text proposed by the Commission

(55a) In light of innovation trends, and the growing accessibility and constantly increasing number of IoT devices in all sectors of society, particular attention must be paid to the security of all and even the simplest of IoT products. Therefore, as certification is a key method for increasing trust in the market and increasing security and resilience, emphasis should be given to IoT products and services in the new EU cybersecurity certification framework, in order to make them less vulnerable and safer for consumers and businesses.

Amendment 21
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 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
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.

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, their inherent risk as well as the intended level of assurance: functionally secure, that is, assurance levels having a functional degree of security, substantially secure, highly secure, or any combination thereof. The assurance levels should not suggest absolute security, so as not to mislead the end-user.

Consideration should also be given to the full lifecycle of the product. In order to clarify which risks a particular product or service is designed to be able to withstand, ENISA should coordinate the compilation of a checklist listing the risks that the ICT process, product or service is expected to face by a given category of users in a particular environment.

Amendment 22

Proposal for a regulation
Recital 56 a (new)

Text proposed by the Commission

(56 a) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services. 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 in respect of establishing European cybersecurity certification schemes for ICT products and services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April
2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council 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. When adopting those delegated acts, the Commission should base the cybersecurity certification schemes for ICT products and services on any relevant candidate schemes proposed by ENISA. In order to underpin trust and predictability in, and raise public awareness of, the cybersecurity certification framework.

Amendment 23
Proposal for a regulation
Recital 56 b (new)

Text proposed by the Commission

(56b) Among the evaluation methods and assessment procedures related to each European cybersecurity certification scheme, ethical hacking, the aim of which is to locate weaknesses and vulnerabilities of devices and information systems by anticipating the intended actions and skills of malicious hackers, should be promoted at Union level.

Amendment 24
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.

With a view to ensuring that accreditation is carried out uniformly across the European Union, national certification supervisory authorities should be subject to a peer review on the procedures for checking the compliance of the products that are subject to cybersecurity certification.

Amendment 25

Proposal for a regulation
Recital 59

Text proposed by the Commission

(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

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. Furthermore, they should supervise and verify the compliance of the self-declarations of conformity and that European cybersecurity certificates have been issued by conformity assessment bodies with the requirements set out in this Regulation including the rules adopted by the European Cybersecurity Certification Group and the requirements set out in the corresponding European cybersecurity certification scheme. 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.

Amendment 26
Proposal for a regulation
Recital 63
Text proposed by the Commission

(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.

Amendment 27

Proposal for a regulation
Recital 65

Text proposed by 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.

Amendment

(65) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT processes, 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).

**Amendment 28**

Proposal for a regulation
Recital 66

*Text proposed by the Commission*

(66) The Agency’s operations should be evaluated independently. The evaluation should have regard to the Agency achieving its objectives, its working practices and the relevance of its tasks. The evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework.

*Amendment*

(66) The Agency’s operations should be evaluated independently. The evaluation should include the legitimacy and effectiveness of the agency’s expenditure, its efficiency in reaching its targets and a description of its working practices and the relevance of its tasks. The evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework.

**Amendment 29**

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

*Text proposed by the Commission*

(11) ‘ICT product and service’ means any element or group of elements of network and information systems;

*Amendment*

(11) ‘ICT process, product and service’ means a product, service, process, system, or a combination thereof that is an element of network and information systems;

(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)

**Amendment 30**

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

*Text proposed by the Commission*

(11 a) “national certification supervisory authority” means an authority of a

*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;

Amendment 31

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

Text proposed by the Commission

(16 a) ‘self-declaration of conformity’ means a statement by the manufacturer that their ICT process, product or service conforms with a specified European cybersecurity certification schemes.

Amendment 32

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 for the purpose of contributing to achieving a high common level of cybersecurity, in order to prevent cyber-attacks within the Union, to reduce fragmentation in the internal market and improve its functioning.

Amendment 33

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. notably in the event of cross-border incidents.

**Amendment 34**

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 *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 Articles 43 to 54 [Title III], with a view to increasing the transparency of cybersecurity assurance of ICT products and services and thus *strengthening* trust in the digital *single* market.

**Amendment 35**

Proposal for a regulation
Article 4 – paragraph 7

*Text proposed by the Commission*

7. The Agency shall promote a high level of awareness of citizens and businesses on issues related to the cybersecurity.

*Amendment*

7. The Agency shall promote a high level of awareness of citizens, *authorities* and businesses on issues related to the cybersecurity.

**Amendment 36**

Proposal for a regulation
Article 5 – paragraph 1 – point 1

*Text proposed by the Commission*

1. assisting and advising, *in particular by providing its independent opinion and*

*Amendment*

1. assisting and advising on the development and review of Union policy
supplying preparatory work, on the
development and review of Union policy
and law in the area of cybersecurity, as
well as sector-specific policy and law
initiatives where matters related to
cybersecurity are involved;

Justification

The agency should be provided with a free choice of instruments to carry out its tasks.

Amendment 37

Proposal for a regulation
Article 5 – paragraph 1 – point 2 a (new)

Text proposed by the Commission  

Amendment

2a. assisting the European Data Protection Board established by Regulation (EU) 2016/679 in developing guidelines to specify at the technical level the conditions allowing the licit use of personal data by data controllers for IT security purposes with the objective of protecting their infrastructure by detecting and blocking attacks against their information systems in the context of: (i) Regulation (EU) 2016/679\(^{1a}\); (ii) Directive (EU) 2016/1148\(^{1b}\); and (iii) Directive 2002/58/EC\(^{1c}\);


\(^{1b}\) (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such...


Justification

Establishing proper cooperation mechanisms.

Amendment 38

Proposal for a regulation
Article 5 – paragraph 1 – point 4 – point 2

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) the promotion of an enhanced level of security of electronic communications, including by providing expertise and advice, as well as facilitating the exchange of best practices between competent authorities;</td>
<td>(2) the promotion of an enhanced level of security of electronic communications, data storage and data processing, including by providing expertise and advice, as well as facilitating the exchange of best practices between competent authorities;</td>
</tr>
</tbody>
</table>

Amendment 39

Proposal for a regulation
Article 6 – paragraph 2 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2a. The Agency shall facilitate the establishment and launch of a long-term European cybersecurity project to support the growth of an independent EU cybersecurity industry, and to mainstream cybersecurity into all EU ICT developments.</td>
<td>2a. The Agency shall facilitate the establishment and launch of a long-term European cybersecurity project to support the growth of an independent EU cybersecurity industry, and to mainstream cybersecurity into all EU ICT developments.</td>
</tr>
</tbody>
</table>
Justification

ENISA should advise legislators regarding the preparation of policies to allow the EU to catch up with IT security industries in third countries. The project should be comparable in scale to what has previously been achieved in the aviation industry (example of Airbus). This is needed to develop a stronger, sovereign and trustworthy EU ICT industry (see the Scientific Foresight Unit (STOA) study PE 614.531).

Amendment 40
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 one 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 41
Proposal for a regulation
Article 7 – paragraph 8 – point a

Text proposed by the Commission

(a) aggregating reports from national sources with a view to contribute to establishing common situational awareness;

Amendment

(a) aggregating reports from national and international sources with a view to contribute to establishing common situational awareness;

Amendment 42
Proposal for a regulation
Article 8 – paragraph 1 – point a – point 1 a (new)

Text proposed by the Commission

(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, with a view to ensuring the uniform application of this Regulation by conformity assessment bodies when issuing certificates;

Amendment 43

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

Text proposed by the Commission

(1 b) carrying out independent periodic ex-post checks on the compliance of certified ICT products and services with European cybersecurity certification schemes;

Amendment 44

Proposal for a regulation
Article 8 – paragraph 1 – point a – point 3

Text proposed by the Commission

(3) compiling and publishing guidelines and developing good practices concerning the cybersecurity requirements of ICT products and services, in cooperation with national certification supervisory authorities and the industry;

(3) compiling and publishing guidelines and developing good practices, including on cyber-hygiene principles and on deterring secret backdoors, concerning the cybersecurity requirements of ICT products and services, in cooperation with national certification supervisory authorities and the industry in a formal, standardised and transparent process;
Amendment 45

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) consult the international standardisation bodies and European standardisation organisations on the development of standards, to ensure the appropriateness of standards used in European Cybersecurity certification schemes and facilitate the establishment and take-up of relevant 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 46

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

Text proposed by the Commission

(b a) draw up guidelines concerning how and when Member States are to inform each other when they acquire knowledge of a vulnerability that is not publicly known in an ICT process, product or service that is certified in accordance with Title III of this Regulation, including guidelines on the coordination of vulnerability disclosure policies;

Amendment

(b a) draw up guidelines concerning how and when Member States are to inform each other when they acquire knowledge of a vulnerability that is not publicly known in an ICT process, product or service that is certified in accordance with Title III of this Regulation, including guidelines on the coordination of vulnerability disclosure policies;
Amendment 47

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

Text proposed by the Commission

(b b) draw up guidelines on minimum security requirements for IT devices placed on the market in the Union or exported from the Union;

Amendment

Amendment 48

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

Text proposed by the Commission

(d) pool, organise and make available to the public, through a dedicated portal, information on cybersecurity, provided by the Union institutions, agencies and bodies;

Amendment

(d) pool, organise and make available to the public, through a dedicated portal, information on cybersecurity, including information about significant cybersecurity incidents and major data breaches, provided by the Union institutions, agencies and bodies;

Amendment 49

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) raise awareness of the public about cybersecurity risks, provide guidance on good practices for users aimed at citizens and organisations and promote the adoption of preventive strong IT security measures and reliable data protection and privacy;

Amendment 50

Proposal for a regulation
Article 9 – paragraph 1 – point g a (new)
Amendment 51

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

Amendment

(g a) support closer cooperation and the exchange of best practices among Member States on cybersecurity education, cyber-hygiene and awareness;

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

Text proposed by the Commission

(a) advise the Union and the Member States on research needs and priorities in the area of cybersecurity, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;

Amendment

(a) ensure prior consultation with relevant user groups and advise the Union and the Member States on research needs and priorities in the area of cybersecurity, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;

Amendment 52

Proposal for a regulation
Article 13 – paragraph 1

Text proposed by the Commission

1. The Management Board shall be composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives shall have voting rights.

Amendment

1. The Management Board shall be composed of one representative of each Member State, and two representatives appointed by the Commission and the European Parliament. All representatives shall have voting rights.

Amendment 53

Proposal for a regulation
Article 14 – paragraph 1 – point e

Text proposed by the Commission

Amendment
e) assess and adopt the consolidated annual report on the Agency’s activities and send both the report and its assessment by 1 July of the following year, to the European Parliament, the Council, the Commission and the Court of Auditors. The annual report shall include the accounts and describe how the Agency has met its performance indicators. The annual report shall be made public;

Amendment 54

Proposal for a regulation
Article 14 – paragraph 1 – point m

Text proposed by the Commission

(m) appoint the Executive Director and where relevant extend his term of office or remove him from office in accordance with Article 33 of this Regulation;

Amendment

(m) appoint the Executive Director through selection based on professional criteria and where relevant extend his term of office or remove him from office in accordance with Article 33 of this Regulation;

Amendment 55

Proposal for a regulation
Article 14 – paragraph 1 – point o

Text proposed by the Commission

o) take all decisions on the establishment of the Agency's internal structures and, where necessary, their modification, taking into consideration the Agency's activity needs and having regard to sound budgetary management;

Amendment

o) take all decisions on the establishment of the Agency's internal structures and, where necessary, their modification, taking into consideration the Agency's activity needs, as listed in this regulation, and having regard to sound budgetary management;

Amendment 56

Proposal for a regulation
Article 19 – paragraph 2
2. The Executive Director shall report to the European Parliament on the performance of his or her duties when invited to do so. The Council may invite the Executive Director to report on the performance of his or her duties.

Amendment 57

Proposal for a regulation
Article 20 – paragraph 1

Text proposed by the Commission

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 Code] as well as of law enforcement and data protection supervisory authorities.

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, and providers of electronic communications networks or services available to the public, in particular European ICT industry and providers, associations of small and medium-sized enterprises, consumer groups and associations, academic experts in the field of cybersecurity, the European standardisation organisations as defined 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.

Amendment 58

Proposal for a regulation
Article 20 – paragraph 4

Text proposed by the Commission

4. The term of office of the Permanent

Amendment

4. The term of office of the Permanent
Stakeholders’ Group’s members shall be two-and-a-half years. Members of the Management Board may not be members of the Permanent Stakeholders’ Group. Experts from the Commission and the Member States shall be entitled to be present at the meetings of the Permanent Stakeholders’ Group and to participate in its work. Representatives of other bodies deemed relevant by the Executive Director, who are not members of the Permanent Stakeholders’ Group, may be invited to attend the meetings of the Permanent Stakeholders’ Group and to participate in its work.

Amendment 59

Proposal for a regulation
Article 20 – paragraph 5

Text proposed by the Commission

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.

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. It may also propose that the Commission request the Agency to prepare candidate European cybersecurity certification schemes in accordance with Article 44, either on its own initiative or following submission of proposals from relevant stakeholders.

Amendment 60

Proposal for a regulation
Article 20 – paragraph 5 a (new)
Text proposed by the Commission

Amendment

5a. The Permanent Stakeholders’ Group shall advise the Agency in the preparation of candidate European Cybersecurity certification schemes.

Amendment 61

Proposal for a regulation
Article 23 – paragraph 2

Text proposed by the Commission

2. The Agency shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 22.

Amendment

2. The Agency shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the debates and the results of its work. It shall also make public the declarations of interest made in accordance with Article 22.

Justification

Transparency needs to be enforceable, taking into account the application of art.24

Amendment 62

Proposal for a regulation
Article 43 – paragraph 1

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

Amendment

A European cybersecurity certification scheme shall be established in order to boost the level of security within the digital single market and adopt a harmonised approach, at EU level, to European certification, with a view to ensuring that ICT products, services and systems are resistant to cyber-attacks. It shall attest that the ICT processes, products and services that have been certified in accordance with such scheme
products, processes, services and systems. comply with specified common requirements and properties as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those processes, products, services and systems.

Amendment 63

Proposal for a regulation

Article 43 a (new)

Text proposed by the Commission

Amendment

Article 43 a

Work Programme

ENISA shall, after consulting the European Cybersecurity Certification Group and the Permanent Stakeholders’ Group and after approval by the Commission, establish a work programme detailing common actions to be undertaken at Union level to ensure the consistent application of this Title, and containing a priority list of ICT products and services for which it considers a European cybersecurity certification scheme to be needed.

The work programme shall be established not later than [six months after entry into force of this Regulation] and a new work programme shall be established every two years thereafter. The work programme shall be made publicly available.

Amendment 64

Proposal for a regulation

Article 44 – paragraph 1
Text proposed by 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 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.

Amendment 65

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 of this Article, ENISA shall consult the Permanent Stakeholders’ Group, in particular the European standardisation organisations and all other relevant stakeholders, including consumer organisations, in a formal, standardised and transparent process, and shall closely cooperate with the Group taking into account already existing national and international standards. When preparing each candidate scheme, ENISA shall establish a checklist of risks and corresponding cybersecurity features.

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 Consultation 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.

Amendment 66
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. ENISA shall transmit the candidate European cybersecurity certification scheme prepared in accordance with paragraph 2 of this Article to the Commission, which shall assess its suitability for achieving the objectives of the request referred to in paragraph 1.

Amendment 67
Proposal for a regulation
Article 44 – paragraph 3 a (new)

Text proposed by the Commission

Amendment
3a. ENISA shall observe professional secrecy with regard to all information obtained in carrying out its tasks under this Regulation.

Amendment 68
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

Amendment
4. The Commission is empowered to adopt delegated acts, in accordance with Article 55a, concerning the establishment of European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46.
meeting the requirements of Articles 45, 46 and 47 of this Regulation. When adopting those delegated acts, the Commission shall base the cybersecurity certification schemes for ICT products and services on any relevant candidate scheme proposed by ENISA. The Commission may consult the European Data Protection Board and take account of its view before adopting such delegated acts.

Amendment 69

Proposal for a regulation
Article 44 – paragraph 5

Text proposed by the Commission

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

Amendment

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.

Amendment 70

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

Text proposed by the Commission

A European cybersecurity certification scheme shall be so designed to take into account, as applicable, the following security objectives:

Amendment

Each European cybersecurity certification scheme shall be so designed as to take into account at least the following security objectives, insofar as they are relevant:

Amendment 71

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

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.

software and hardware that does not contain known vulnerabilities; ensure that they have been designed and implemented in such a way as to effectively limit their susceptibility to vulnerabilities, and ensure that they are provided with mechanisms for secure software updates, including upgrades of hardware and automatic security updates;

Amendment 72

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

Text proposed by the Commission

(g a) ensure that ICT products and services are developed and operated in such a way that a high level of cybersecurity and data protection is preconfigured, in accordance with the principle of “security by design”.

Amendment

Amendment 73

Proposal for a regulation
Article 46 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Each European cybersecurity certification scheme may specify one or more of the following risk-based assurance levels: “functionally secure”; “substantially secure” and/or “highly secure”, for ICT products and services issued under that scheme.

The assurance levels for each candidate European cybersecurity certification scheme shall be identified on the basis of the risks identified in the checklist established in Article 44(2) and the availability of cybersecurity features to counter those risks in the ICT products and services to which the certification
scheme applies.

Amendment 74

Proposal for a regulation
Article 46 – paragraph 1 a (new)

Text proposed by the Commission

1 a. Each scheme shall indicate the assessment methodology or evaluation process that is to be followed for issuing certificates at each assurance level, depending on the intended use and the risk inherent to the ICT products and services under that scheme.

Amendment

Amendment 75

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

Text proposed by the Commission

2. The assurance levels basic, substantial and high shall meet the following criteria respectively:

Amendment

2. The assurance levels “functionally secure”, “substantially secure” and/or “highly secure” shall meet the following criteria respectively:

Amendment 76

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,

Amendment

(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 process, product or service, and is characterised with reference to technical specifications, standards and procedures
including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents;

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

Amendment 77

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 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;

Amendment

(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 **process**, 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;

Amendment 78

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

Amendment

(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 **process**, product or service than certificates with the assurance level **substantially secure**, and is characterised with reference to technical specifications, standards and procedures related thereto,
controls, the purpose of which is to prevent cybersecurity incidents. including technical controls, the purpose of which is to prevent cybersecurity incidents. This shall apply in particular to products and services intended for use by operators of essential services, as defined in Art 4(4) of Directive 2016/1148/EU.

Amendment 79

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

Text proposed by the Commission

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

Amendment

1. Each European cybersecurity certification scheme shall include at least the following elements, where applicable:

Amendment 80

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 scheme, including any specific sectors covered, and the type or categories of ICT products and services covered;

Amendment 81

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

Text proposed by the Commission

(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;

Amendment

(b) detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, in particular by reference to international, European, or national standards or technical specifications;
Amendment 82
Proposal for a regulation
Article 47 – paragraph 1 – point b a (new)

Text proposed by the Commission

(b a) detailed specification if a granted certification can apply to only an individual product or can be applied to a product range, for example different versions or models of the same base product structure;

Amendment 83
Proposal for a regulation
Article 47 – paragraph 1 – point c a (new)

Text proposed by the Commission

(c a) indication of whether self-declaration of conformity is permitted under the scheme, and the applicable procedure for conformity assessment or self-declaration of conformity or both;

Amendment 84
Proposal for a regulation
Article 47 – paragraph 1 – point c b (new)

Text proposed by the Commission

(c b) certification requirements defined in such a way that certification can be incorporated into or based on the producer’s systematic cybersecurity processes followed during the design, development and lifecycle of the ICT process, product or service;

Amendment 85
Proposal for a regulation
Article 47 – paragraph 1 – point f

Text proposed by the Commission

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

Amendment

(f) where the scheme provides for marks or labels, such as an EU *Cybersecurity Conformity label signifying that an ICT process, product or service complies with the criteria of a scheme*, the conditions under which such marks or labels may be used;

Amendment 86

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

Text proposed by the Commission

(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;

Amendment

(g) the rules for monitoring compliance with the requirements of the certificates, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements *such as, where relevant and feasible, obligatory updates, upgrades or patches of the concerned ICT process, product or service*;

Amendment 87

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

Text proposed by the Commission

(h) conditions for granting, maintaining, continuing, extending and reducing the scope of certification;

Amendment

(h) conditions for granting, maintaining, continuing, *renewing*, extending and reducing the scope of certification;

Amendment 88

Proposal for a regulation
Article 47 – paragraph 1 – point i
Text proposed by the Commission

(i) rules concerning the consequences of non-conformity of certified ICT products and services with the certification requirements;

Amendment

(i) rules concerning the consequences of non-conformity of certified ICT products and services with the certification requirements, and general information on penalties, as laid down in Article 54 of this Regulation;

Amendment 89

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

Text proposed by the Commission

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

Amendment

(j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with, including through coordinated vulnerability disclosure processes;

Amendment 90

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

Text proposed by the Commission

(l) identification of national cybersecurity certification schemes covering the same type or categories of ICT products and services;

Amendment

(l) identification of national or international cybersecurity certification schemes, or existing international mutual recognition agreements, covering the same type or categories of ICT products and services;

Amendment 91

Proposal for a regulation
Article 47 – paragraph 1 – point m a (new)
Amendment 92

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

Text proposed by the Commission

(m b) rules concerning resistance and resilience testing for the “highly secure” assurance level.

Amendment 93

Proposal for a regulation
Article 47 – paragraph 3

Text proposed by the Commission

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

Amendment 94

Proposal for a regulation
Article 48 – paragraph 2

Text proposed by the Commission

2. Certification under a European cybersecurity certification scheme shall be mandatory for ICT products and services with a high inherent risk that are specifically intended for use by operators of essential services, as defined in Article 4(4) of Directive 2016/1148/EU. For all other ICT products and services

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

Amendment 95
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. European cybersecurity **certificates** 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.

As an alternative to certification by conformity assessment bodies, product manufacturers and service providers may, where the scheme in question provides for such a possibility, make a self-declaration of conformity in which they declare that a process, product or service complies with the criteria of the certification scheme. In such cases, the product manufacturer or service provider shall, upon request, provide the self-declaration of conformity to the requesting national certification supervisory authority and ENISA.

Amendment 96
Proposal for a regulation
Article 48 – paragraph 4 – introductory part

Text proposed by the Commission

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

Amendment

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

Amendment 97

Proposal for a regulation
Article 48 – paragraph 5

Text proposed by the Commission

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.

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, including information on any known security vulnerabilities.

Amendment 98

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 and shall remain valid for a maximum period defined in each certification scheme and may be renewed, under the same conditions, provided that the relevant requirements of that scheme, including any revised or amended requirements, continue to be met.

Amendment 99

Proposal for a regulation
Article 48 – paragraph 6 a (new)

Text proposed by the Commission

6 a. Certificates shall remain valid for all new versions of a process, product or service, where the primary reason for the new version is to patch, fix, or otherwise
address known or potential security vulnerabilities or threats.

Amendment 100
Proposal for a regulation
Article 49 – paragraph 1

Text proposed by the Commission

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

Amendment

1. Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the delegated act adopted pursuant to Article 44(4). The Commission shall monitor compliance with this subparagraph, in order to avoid the existence of concurrent schemes. Existing national cybersecurity certification schemes and the related procedures for the ICT products and services not covered by a European cybersecurity certification scheme shall continue to exist.

Amendment 101
Proposal for a regulation
Article 49 – paragraph 3

Text proposed by the Commission

3. Existing certificates issued under national cybersecurity certification schemes shall remain valid until their expiry date.

Amendment

3. Existing certificates issued under national cybersecurity certification schemes that are covered by a European cybersecurity certification scheme shall remain valid until their expiry date.

Amendment 102
Proposal for a regulation
Article 50 – paragraph 3
3. Each national certification supervisory authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise.

Amendment 103

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

Text proposed by the Commission

(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;

Amendment

(a) monitor and enforce the application of the provisions under this Title at national level and supervise compliance, in accordance with the rules adopted by the European Cybersecurity Certification Group pursuant to point (da) of Article 53(3), of:

i) 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; and

ii) self-declarations of conformity made under a scheme for an ICT process, product or service;

Amendment 104

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

Text proposed by the Commission

(b) monitor and supervise the activities of conformity assessment bodies for the purpose of this Regulation, including in

Amendment

(b) monitor, supervise and, at least every two years, assess the activities of conformity assessment bodies for the
relation to the notification of conformity assessment bodies and the related tasks set out in Article 52 of this Regulation;

Amendment 105

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

Text proposed by the Commission

(c) handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories, investigate, to the extent appropriate, the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation within a reasonable time period;

Amendment

(c) handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories or to self-declarations of conformity made, 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;

Amendment 106

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

Text proposed by the Commission

(c a) report the results of verifications under point (a) and the assessments under points (b) to ENISA and the European Cybersecurity Certification Group;

Amendment

(c a) report the results of verifications under point (a) and the assessments under points (b) to ENISA and the European Cybersecurity Certification Group;

Amendment 107

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

Text proposed by the Commission

(d) cooperate with other national certification supervisory authorities or

Amendment

(d) cooperate with other national certification supervisory authorities,
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;

**Amendment 108**

Proposal for a regulation  
Article 50 – paragraph 7 – point c a (new)

*Text proposed by the Commission*

**Amendment**

(c a) to revoke the accreditation of conformity assessment bodies that do not comply with this Regulation;

**Amendment 109**

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

*Text proposed by the Commission*

(e) to withdraw, in accordance with national law, certificates that are not compliant with this Regulation or a European cybersecurity certification scheme;  

**Amendment**

(e) to withdraw, in accordance with national law, certificates that are not compliant with this Regulation or a European cybersecurity certification scheme and inform national accreditation bodies accordingly;

**Amendment 110**

Proposal for a regulation  
Article 50 – paragraph 7 – point f a (new)

*Text proposed by the Commission*

**Amendment**

(f a) to suggest ENISA experts who could be part of the Stakeholder Consultation expert group, referred to in Article 44(2).
Amendment 111

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

Text proposed by the Commission

The Commission shall make available a general electronic information support system for the purpose of that exchange.

Amendment 112

Proposal for a regulation
Article 50 a (new)

Text proposed by the Commission

Article 50 a

Peer review

1. National certification supervisory authorities shall be subject to peer review in respect of any activity which they carry out pursuant to Article 50 of this Regulation.

2. Peer review shall cover the assessments of the procedures put in place by national certification supervisory authorities, in particular the procedures for checking the compliance of the products that are subject to cybersecurity certification, the competence of the personnel, the correctness of the checks and the inspection methodology as well as the correctness of the results. Peer review shall also assess whether national certification supervisory authorities in question have sufficient resources for the proper performance of their duties as required by Article 50(4).

3. Peer review of a national certification supervisory authority shall be carried out by two national certification supervisory authorities of other Member
States and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review and shall decide on its participation on the basis of a risk assessment analysis.

4. The Commission is empowered, in accordance with Article 55a, to adopt delegated acts, in order to establish a plan for the peer review covering a period of at least five years, laying down criteria concerning the composition of the peer review team, the methodology used for the peer review, the schedule, periodicity and the other tasks related to the peer review. When adopting those delegated acts, the Commission shall take due account of the considerations of the Group.

5. The outcome of the peer review shall be examined by the Group. ENISA shall draw up a summary of the outcome and make it public.

Amendment 113
Proposal for a regulation
Article 51 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. Where manufacturers opt for ‘self-declaration of conformity’ in accordance with Article 48(3), conformity assessment bodies shall take additional steps to verify the internal procedures undertaken by the manufacturer to ensure that their products and/or services conform with the requirements of the European cybersecurity certification scheme.

Amendment 114
Proposal for a regulation
Article 53 – paragraph 3 – point d a (new)
Text proposed by the Commission

(d a) to adopt binding rules determining the intervals at which national certification supervisory authorities are to carry out verifications of certificates and self-declarations of conformity, and the criteria, scale and scope of those verifications and to adopt common rules and standards for reporting, in accordance with Article 50(6);

Amendment 115
Proposal for a regulation
Article 53 – paragraph 3 – point e

Text proposed by the Commission

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

Amendment 116
Proposal for a regulation
Article 53 – paragraph 3 – point f a (new)

Text proposed by the Commission

(f a) to exchange best practices in relation to investigations of conformity assessment bodies, European cybersecurity certificate holders and manufacturers and service providers that have made self-declarations of conformity;

Amendment 117
Proposal for a regulation
Article 53 – paragraph 3 – point f b (new)
Amendment 118

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

(f c) to advise ENISA, when establishing the Work Programme referred to in Article 43a, on a priority list of ICT products and services for which it considers a European cybersecurity certification scheme to be needed;

Amendment 119

Proposal for a regulation
Article 53 – paragraph 4 – subparagraph 1 a (new)

ENISA shall ensure that the agenda, minutes and a record of decisions taken are registered and that published versions of those documents are made available to the public on the ENISA website after each meeting of the Group.

Amendment 120

Proposal for a regulation
Article 55 a (new)
Article 55a

Exercise of the delegation

The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

The power to adopt delegated acts referred to in Articles 44(4) and 50a(4) shall be conferred on the Commission for a period of 5 years from [date of entry into force of the basic legislative act]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the 5 year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

The delegation of power referred to in Articles 44(4) and 50a(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

A delegated act adopted pursuant to Article 44(4) or 50a(4) shall enter into
force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.
### PROCEDURE – COMMITTEE ASKED FOR OPINION

<table>
<thead>
<tr>
<th>Title</th>
<th>Regulation on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (’Cybersecurity Act’’)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee responsible</td>
<td>ITRE 23.10.2017</td>
</tr>
<tr>
<td>Opinion by</td>
<td>IMCO 23.10.2017</td>
</tr>
<tr>
<td>Associated committees - date announced in plenary</td>
<td>18.1.2018</td>
</tr>
<tr>
<td>Rapporteur</td>
<td>Nicola Danti 25.9.2017</td>
</tr>
<tr>
<td>Discussed in committee</td>
<td>21.2.2018 21.3.2018</td>
</tr>
<tr>
<td>Date adopted</td>
<td>17.5.2018</td>
</tr>
</tbody>
</table>
| Result of final vote | +: 31  
-: 2  
0: 1 |
| Members present for the final vote | John Stuart Agnew, Pascal Arimont, Dita Charanzová, Carlos Coelho, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Dennis de Jong, Pascal Durand, Evelyne Gebhardt, Robert Jaroslaw Iwaszkiewicz, Liisa Jaakonsaari, Marlene Mizzi, Nosheena Mobarak, Jiří Pospíšil, Andreas Schwab, Olga Sehnalová, Jasenko Selimovic, Ivan Štefanec, Catherine Stihler, Mylène Troszczynski, Mihai Țurcanu, Anneleen Van Bossuyt, Marco Zullo |
| Substitutes present for the final vote | Jan Philipp Albrecht, Kaja Kallas, Arndt Kohn, Emma McClarkin, Adam Szejnfeld, Marc Tarabella, Lambert van Nistelrooij, Kerstin Westphal |
| Substitutes under Rule 200(2) present for the final vote | Inés Ayala Sender, Flavio Zanonato |
### FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>ALDE</td>
<td>Dita Charanzová, Kaja Kallas, Jasenko Selimovic</td>
<td></td>
</tr>
<tr>
<td>ECR</td>
<td>Daniel Dalton, Emma McClarkin, Nosheena Mobarik, Anneleen Van Bossuyt</td>
<td></td>
</tr>
<tr>
<td>EFDD</td>
<td>Marco Zullo</td>
<td></td>
</tr>
<tr>
<td>GUE/NGL</td>
<td>Dennis de Jong</td>
<td></td>
</tr>
<tr>
<td>PPE</td>
<td>Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Jiří Pospíšil, Andreas Schwab, Ivan Štefanec, Adam Szejnfeld, Mihai Ţurcanu, Lambert van Nistelrooij</td>
<td></td>
</tr>
<tr>
<td>S&amp;D</td>
<td>Inés Ayala Sender, Nicola Danti, Evelyne Gebhardt, Liisa Jaakonsaari, Arndt Kohn, Marlene Mizzi, Olga Sehnalová, Catherine Stihler, Marc Tarabella, Kerstin Westphal, Flavio Zanonato</td>
<td></td>
</tr>
<tr>
<td>Verts/ALE</td>
<td>Jan Philipp Albrecht, Pascal Durand</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>EFDD</td>
<td>John Stuart Agnew, Robert Jarosław Iwaszkiewicz</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ENF</td>
<td>Mylène Troszczynski</td>
<td></td>
</tr>
</tbody>
</table>

**Key to symbols:**
- + : in favour
- - : against
- 0 : abstention