

AMENDMENTS 001-257

by the Committee on Industry, Research and Energy

Report**Angelika Niebler**

EU Cybersecurity Act

A8-0264/2018

Proposal for a regulation (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

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

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.

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, *processes* and services, undermining trust in digital solutions. ***This ambition is at the heart of the European Commission's reform agenda to achieve a digital single market as ICT networks provide the backbone for digital products and services which have the potential to support all aspects of our lives and drive Europe's economic growth. To ensure that the objectives of the digital single market are fully achieved the essential technology building blocks on which important areas such as eHealth, IoT, Artificial Intelligence, Quantum technology as well as intelligent transport system and advanced manufacturing rely must be in place.***

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

Amendment

(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.

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. ***In this respect the Digital Education Action Plan published by the European Commission on 17 January 2018 is a step in the right direction, in particular the EU-wide awareness-raising campaign targeting educators, parents and learners to foster online safety, cyber hygiene and media literacy as well as the cyber-security teaching initiative building on the Digital Competence Framework for Citizens, to empower people to use technology confidently and responsibly.***

Amendment 4

Proposal for a regulation Recital 3 a (new)

Text proposed by the Commission

Amendment

(3 a) Believes that the objectives and tasks of ENISA should be further aligned with the Joint Communication with regards to its reference to the promotion of cyber hygiene and awareness; notes that cyber resilience can be achieved by implementing basic cyber hygiene principles;

Amendment 5

Proposal for a regulation Recital 3 b (new)

Text proposed by the Commission

Amendment

(3b) ENISA should give more practical and information-based support to the Union cybersecurity industry, in particular SMEs and start-ups, which are key sources of innovative solutions in the

area of cyber defence, and should promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cybersecurity products from external sources and to creating a strategic supply chain inside the Union.

Amendment 6

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

(4) Cyber-attacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger ***and more secure*** 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. ***Training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at Union level.*** 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 7

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 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.

Amendment

(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination *and information sharing* 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, *while underlining the importance of maintaining and further enhancing the national capabilities to respond to cyber threats of all scales* Additional efforts are also needed to *deliver a co-ordinated EU response and* increase awareness of citizens and businesses on cybersecurity issues. Moreover, *given that cyber incidents undermine trust in digital service providers and* in the digital single market *itself, especially among consumers, trust* should be further improved by offering transparent information on the level of security of ICT products, *processes and services stressing that even a high level of cybersecurity certification cannot guarantee an ICT product or service is completely safe.* This can be facilitated by EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors *as well as promoting cyber literacy* *Alongside Union-wide certification and given the growing availability of IoT devices, there are a range of voluntary measures that the private sector should take to reinforce trust in the security of ICT products, processes and services, such as encryption*

and block chain technologies. The challenges faced should be proportionally reflected in the budget allocated to the Agency, so as to ensure the optimal functionality under the current circumstances.

Amendment 8

Proposal for a regulation Recital 5 a (new)

Text proposed by the Commission

Amendment

(5 a) For the purpose of strengthening European security and cyber defence structures, it is important to maintain and develop the capabilities of Member States to comprehensively respond to cyber threats, including cross-border incidents while coordination on EU-level by the Agency should not lead to the diminishing of capabilities or efforts in the Member States.

Amendment 9

Proposal for a regulation Recital 5 b (new)

Text proposed by the Commission

Amendment

(5b) Businesses as well as individual consumers should have accurate information regarding the level of security of their ICT products. At the same time, it has to be understood that no product is cyber secure and that basic rules of cyber hygiene have to be promoted and prioritised.

Amendment 10

Proposal for a regulation Recital 7

(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.

(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 depends heavily on the effective implementation by Member States, fulfils the digital single market strategy and together with other instruments, such as the Directive establishing the European Electronic Communications Code, Regulation (EU) 2016/679 and Directive 2002/58/EC, puts* 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 introduces 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 11

Proposal for a regulation

Recital 8

Text proposed by the Commission

(8) It is recognised that, since the adoption of the 2013 EU Cybersecurity Strategy and the last revision of the Agency's mandate, the overall policy context has changed significantly, also in relation to a more uncertain and less secure global environment. In this context and within the framework of the new Union cybersecurity policy, it is necessary to review the mandate of ENISA to define its role in the changed cybersecurity ecosystem and ensure it contributes effectively to the Union's response to cybersecurity challenges emanating from this radically transformed threat landscape, for which, as recognised by the evaluation of the Agency, the current mandate is not sufficient.

Amendment

(8) It is recognised that, since the adoption of the 2013 EU Cybersecurity Strategy and the last revision of the Agency's mandate, the overall policy context has changed significantly, also in relation to a more uncertain and less secure global environment. In this context ***and in the context of the positive role the Agency has played over the years in the pooling of expertise, coordination, capacity building*** and within the framework of the new Union cybersecurity policy, it is necessary to review the mandate of ENISA to define its role in the changed cybersecurity ecosystem and ensure it contributes effectively to the Union's response to cybersecurity challenges emanating from this radically transformed threat landscape, for which, as recognised by the evaluation of the Agency, the current mandate is not sufficient.

Amendment 12

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, ***allowing ENISA to effectively carry out the tasks conferred on it by this Regulation.***

Amendment 13

Proposal for a regulation

Recital 12

Text proposed by the Commission

(12) The Agency should develop and maintain a high level of expertise and operate as a point of reference establishing trust and confidence in the single market by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in carrying out its tasks. The Agency should proactively contribute to national and Union efforts while carrying out its tasks in full cooperation with the Union institutions, bodies, offices and agencies and the Member States. In addition, the Agency should build on input from and cooperation with the private **sector** as well as other relevant stakeholders. A set of tasks should establish how the Agency is to accomplish its objectives while allowing flexibility in its operations.

Amendment

(12) The Agency should develop and maintain a high level of expertise and operate as a point of reference establishing trust and confidence in the single market by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in carrying out its tasks. The Agency should proactively contribute to national and Union efforts while carrying out its tasks in full cooperation with the Union institutions, bodies, offices and agencies and the Member States, ***avoiding any duplication of work, promoting synergy and complementarity and thus achieving coordination and fiscal savings.*** In addition, the Agency should build on input from and cooperation with the private ***and public sectors*** as well as other relevant stakeholders. A ***clear agenda and a set of tasks and objectives which should be clearly defined*** should establish how the Agency is to accomplish its objectives while ***giving due consideration to the necessary flexibility of its operations.*** ***Where possible, the highest degree of transparency and dissemination of information should be maintained.***

Amendment 14

Proposal for a regulation
Recital 12 a (new)

Text proposed by the Commission

Amendment

(12 a) The role of the Agency should be subject to a continuous assessment and a timely review, in particular its coordinating role vis-à-vis the Member States and their national authorities and the possibility of acting as a One-Stop-Shop for Member States and EU bodies and institutions. The Agency's role in the avoidance of the fragmentation of the

internal market and the possible introduction of mandatory cybersecurity certification schemes, should the situation in the future require such a shift, should also be assessed as well as the Agency's role in respect of the assessment of third country products entering the EU market and the possible blacklisting of companies which do not comply with EU criteria.

Amendment 15

Proposal for a regulation Recital 12 b (new)

Text proposed by the Commission

Amendment

(12b) In order to be able to provide adequate support to the operational cooperation to the Member States, ENISA should further strengthen its own technical capabilities and expertise. For this purpose the Agency should progressively reinforce its staff dedicated to this task so as to be able to collect and analyse autonomously different types of a wide range of cybersecurity threats and malware, perform forensic analysis and assist Member States in the response to large scale incidents. In order to avoid any duplication of existing capabilities in the Member States, ENISA should increase its know-how and capacities based on existing resources present in the Member States, notably by seconding national experts to the Agency, creating pools of experts, staff- exchange programmes etc. When selecting staff responsible in this area, the Agency should progressively ensure that they meet the appropriate criteria to provide adequate support.

Amendment 16

Proposal for a regulation Recital 13

Text proposed by the Commission

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

Amendment

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

Amendment 17

Proposal for a regulation Recital 14

Text proposed by the Commission

(14) The underlying task of the Agency is to promote the consistent implementation of the relevant legal framework, in particular the effective implementation of the NIS Directive, which is essential in order to increase cyber resilience. In view of the fast evolving cybersecurity threat landscape, it is clear that Member States must be supported by more comprehensive, cross-policy approach to building cyber resilience.

Amendment

(14) The underlying task of the Agency is to promote the consistent implementation of the relevant legal framework, in particular the effective implementation of the NIS Directive, ***the Directive establishing the European Electronic Communications Code, Regulation (EU) 2016/679 and Directive 2002/58/EC***, which is essential in order to increase cyber resilience. In view of the fast evolving cybersecurity threat landscape, it is clear that Member States must be supported by more comprehensive, cross-policy

approach to building cyber resilience.

Amendment 18

Proposal for a regulation

Recital 15

Text proposed by the Commission

(15) The Agency should assist the Member States and Union institutions, bodies, offices and agencies in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cybersecurity problems and incidents and in relation to the security of network and information systems. In particular, the Agency should support the development and enhancement of national CSIRTs, with a view of achieving a high common level of their maturity in the Union. The Agency should also assist with the development and update of Union and Member States strategies on the security of network and information systems, in particular on cybersecurity, promote their dissemination and track progress of their implementation. The Agency should also offer trainings and training material to public bodies, and *where appropriate* "train the trainers" with a view to assisting Member States in developing their own training capabilities.

Amendment

(15) The Agency should assist the Member States and Union institutions, bodies, offices and agencies in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cybersecurity problems and incidents and in relation to the security of network and information systems. In particular, the Agency should support the development and enhancement of national CSIRTs, with a view of achieving a high common level of their maturity in the Union. The Agency should also assist with the development and update of Union and Member States strategies on the security of network and information systems, in particular on cybersecurity, promote their dissemination and track progress of their implementation. ***Considering that human mistakes are one of the most pertinent risks to cyber security***, the Agency should also offer trainings and training material to public bodies, and ***to the maximum extent possible*** "train the trainers" with a view to assisting Member States ***and Union institutions and agencies*** in developing their own training capabilities. ***The Agency should also serve as a contact point for Member States and Union institutions, who should be able to request the assistance of the Agency within the competences and roles assigned to it.***

Amendment 19

Proposal for a regulation

Recital 18

Text proposed by the Commission

(18) The Agency should aggregate and analyse national reports from CSIRTs and CERT-EU, setting up common rules, language and terminology for exchange of information. The Agency should also involve the private **sector**, within the framework of the NIS Directive which laid down the grounds for voluntary technical information exchange at the operational level with the creation of the CSIRTs Network.

Amendment

(18) The Agency should aggregate and analyse national reports from CSIRTs and CERT-EU, setting up common rules, language and terminology for exchange of information. The Agency should also involve the private **and public sectors**, within the framework of the NIS Directive which laid down the grounds for voluntary technical information exchange at the operational level with the creation of the CSIRTs Network.

Amendment 20

Proposal for a regulation

Recital 19

Text proposed by the Commission

(19) The Agency should contribute to an EU level response in case of large-scale cross-border cybersecurity incidents and crises. This function should include gathering relevant information and acting as facilitator between the CSIRTs Network and the technical community as well as decision makers responsible for crisis management. Furthermore, the Agency could support the handling of incidents from a technical perspective by facilitating relevant technical exchange of solutions between Member States and by providing input into public communications. The Agency should support the process by testing modalities of such cooperation through yearly cybersecurity exercises.

Amendment

(19) The Agency should contribute to an EU level response in case of large-scale cross-border cybersecurity incidents and crises. This function should include ***convening Member States' authorities and assisting in the coordination of their response***, gathering relevant information and acting as facilitator between the CSIRTs Network and the technical community as well as decision makers responsible for crisis management. Furthermore, the Agency could support the handling of incidents from a technical perspective, ***for example*** by facilitating relevant technical exchange of solutions between Member States and by providing input into public communications. The Agency should support the process by testing modalities of such cooperation through yearly cybersecurity exercises. ***The Agency should respect the competences of the Member States regarding cybersecurity, especially those concerning public security, defence, national security and the activities of the state in areas of criminal law.***

Amendment 21

Proposal for a regulation Recital 25

Text proposed by the Commission

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

Amendment

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

Amendment 22

Proposal for a regulation Recital 26

Text proposed by the Commission

(26) To understand better the challenges in the field of cybersecurity, and with a view to providing strategic long term advice to Member States and Union institutions, the Agency needs to analyse current and emerging risks. For that purpose, the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information and perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on network and information security, in particular cybersecurity. The Agency should furthermore support Member States and Union institutions, agencies and bodies in identifying emerging trends and preventing problems related to cybersecurity, by performing analyses of threats **and** incidents.

Amendment

(26) To understand better the challenges in the field of cybersecurity, and with a view to providing strategic long term advice to Member States and Union institutions, the Agency needs to analyse current and emerging risks, **incidents, threats and vulnerabilities**. For that purpose, the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information and perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on network and information security, in particular cybersecurity. The Agency should furthermore support Member States and Union institutions, agencies and bodies in identifying emerging trends and preventing problems related to cybersecurity, by performing analyses of threats, incidents **and vulnerabilities**.

Amendment 23

Proposal for a regulation
Recital 27

Text proposed by the Commission

(27) In order to increase the resilience of the Union, the Agency should develop excellence on the subject of security of internet infrastructure and of the critical infrastructures, by providing advice, guidance and best practices. With a view to ensuring easier access to better structured information on cybersecurity risks and potential remedies, the Agency should develop and maintain the "information hub" of the Union, a one-stop-shop portal providing the public with information on cybersecurity deriving from the EU and national institutions, agencies and bodies.

Amendment

(27) In order to increase the resilience of the Union, the Agency should develop excellence on the subject of security of internet infrastructure and of the critical infrastructures, by providing advice, guidance and best practices. With a view to ensuring easier access to better structured information on cybersecurity risks and potential remedies, the Agency should develop and maintain the "information hub" of the Union, a one-stop-shop portal providing the public with information on cybersecurity deriving from the EU and national institutions, agencies and bodies. ***Facilitating access to better structured information on cybersecurity risks and potential remedies should help Member States bolster their capacities and align their practices, hence increasing their overall resilience in the face of cyber-attacks.***

Amendment 24

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

Amendment

(28) The Agency should contribute towards raising the awareness of the public, ***including by promoting education,*** about cybersecurity ***risks*** and provide guidance on good practices for individual users aimed at citizens, organisations ***and businesses.*** The Agency should also contribute to promote ***cyber hygiene*** best practices, ***which covers several practices that should be implemented and carried out regularly to protect users and businesses online,*** and solutions at the level of individuals organisations ***and businesses*** by collecting and analysing publicly available information regarding

organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting basic authentication and data protection advice. The Agency should play a central role in accelerating end-user awareness on security of devices.

significant incidents, and by compiling **and publishing reports and guides** with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. **ENISA should also strive to provide consumers with relevant information on applicable certification schemes, for example by providing guidelines and recommendations to online and offline marketplaces.** The Agency should furthermore organise, **in line with the Digital Education Action Plan and** 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, **digital literacy** and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting basic **multi-factor authentication, patching, encryption, anonymisation** and data protection advice. The Agency should play a central role in accelerating end-user awareness on security of devices **and secure use of services, popularising at EU level security-by-design, privacy-by-design, the incidents and their solutions. In achieving this objective the Agency needs to make best use of available best practices and experience, especially academic institutions and IT security researchers. Given that individual mistakes and unawareness of cybersecurity risks constitutes a main factor of uncertainty in cyber security, the Agency should be provided with adequate resources for exercising this function to the fullest degree possible.**

Amendment 25

Proposal for a regulation Recital 28 a (new)

(28a) The Agency should raise public awareness of the risks of data fraud incidents and thefts that may seriously affect individuals' fundamental rights, pose a threat to the rule of law and endanger the stability of democratic societies including democratic processes in the Member States.

Amendment 26

Proposal for a regulation

Recital 30

Text proposed by the Commission

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

Amendment

(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, ***EU supervisory and other competent authorities***, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European ***GNSS Agency (GSA), Body of European Regulators for Electronic Communications (BEREC), European Agency for the operational management of large-scale IT systems (eu-LISA), European Central Bank (ECB), European Banking Authority (EBA), European Data Protection Board (EDPB)***, European Aviation Safety Agency (EASA) and any other EU Agency that is involved in cybersecurity. It should also liaise with ***European Standards Organisations (ESOs), relevant stakeholders and*** authorities dealing with data protection in order to exchange know-how and best practices and provide advice on cybersecurity aspects that might have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the ***ENISA Advisory*** Group. In liaising with law enforcement bodies regarding network and

information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks.

Partnerships should be established with academic institutions that have research initiatives in the relevant areas, while the input from consumer organisations and other organisations should have appropriate channels and should always be analysed.

Amendment 27

Proposal for a regulation

Recital 31

Text proposed by the Commission

(31) The Agency, as a Member which furthermore provides the Secretariat of the CSIRTs Network, should support Member State CSIRTs and the CERT-EU in operational cooperation further to all the relevant tasks of the CSIRTs Network, as defined by the NIS Directive. Furthermore, the Agency should promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or protected by the CSIRTs and involving or potentially involving at least two CERTs while taking due account of the Standard Operating Procedures of the CSIRTs Network.

Amendment

(31) The Agency, as a Member which furthermore provides the Secretariat of the CSIRTs Network, should support Member State CSIRTs and the CERT-EU in operational cooperation further to all the relevant tasks of the CSIRTs Network, as defined by the NIS Directive. Furthermore, the Agency should promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or protected by the CSIRTs and involving or potentially involving at least two CERTs while taking due account of the Standard Operating Procedures of the CSIRTs Network. ***The Agency may, on request by the Commission or a Member State, conduct regular IT security audits of critical cross-border infrastructures with the objective of identifying possible cybersecurity risks and with a view to identifying recommendations to strengthen their resilience.***

Amendment 28

Proposal for a regulation

Recital 33

Text proposed by the Commission

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

Amendment

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

Amendment 29

Proposal for a regulation

Recital 35

Text proposed by the Commission

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

Amendment

(35) The Agency should encourage Member States, ***manufacturers*** and service providers to raise their general security standards ***of their ICT products, processes, services and systems which should comply with basic security obligations in line with the principle of security by design and by default, in particular by providing necessary updates***, so that all internet users can ***be secured and incentivised to*** take the necessary steps to ensure their own personal cybersecurity. In particular, service providers and product manufacturers should ***recall***, withdraw or recycle products and services that do not meet ***basic*** cybersecurity ***obligations, while importers and distributors should make sure that ICT products, processes, services and systems they place on the EU market comply with the applicable requirements and do not present a risk to European consumers***. 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, manufacturers and requiring them to improve the security, including cybersecurity, of their products, *processes, services and systems. The Agency should work together with stakeholders towards developing a EU-wide approach to responsible vulnerabilities disclosure and should promote best practices in this area.*

Amendment 30

Proposal for a regulation Recital 36

Text proposed by the Commission

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

Amendment

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

Amendment 31

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 Agency should regularly consult and work in close cooperation with the standardisation organisations, in particular when preparing the European Cybersecurity Certification Schemes.

Amendment 32

Proposal for a regulation

Recital 37

Text proposed by the Commission

(37) Cybersecurity problems are global issues. There is a need for closer international cooperation to improve security standards, including the definition of common norms of behaviour, and information sharing, promoting swifter international collaboration in response to, as well as a common global approach to, network and information security issues. To that end, the Agency should support further Union involvement and cooperation with third countries and international organisations by providing, where appropriate, the necessary expertise and analysis to the relevant Union institutions, bodies, offices and agencies.

Amendment

(37) Cybersecurity problems are global issues. There is a need for closer international cooperation to improve security standards, including the definition of common norms of behaviour ***and codes of conduct, use of international standards***, and information sharing, promoting swifter international collaboration in response to, as well as a common global approach to, network and information security issues. To that end, the Agency should support further Union involvement and cooperation with third countries and international organisations by providing, where appropriate, the necessary expertise and analysis to the relevant Union institutions, bodies, offices and agencies.

Amendment 33

Proposal for a regulation

Recital 40

Text proposed by the Commission

(40) The Management Board, ***composed of*** the Member States and the Commission, should define the general direction of the Agency's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial

Amendment

(40) The Management Board, ***representing*** the Member States and the Commission ***as well as stakeholders relevant for the Agency's objectives***, should define the general direction of the Agency's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers

rules, establish transparent working procedures for decision making by the Agency, adopt the Agency's Single Programming Document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.

necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, adopt the Agency's Single Programming Document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof. ***In light of the highly technical and scientific tasks of the Agency, members of the Management Board should have appropriate experience and a high level of expertise in issues within the scope of the Agency's missions.***

Amendment 34

Proposal for a regulation Recital 41

Text proposed by the Commission

(41) In order for the Agency to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Management Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Management Board in order to ensure continuity in its work.

Amendment

(41) In order for the Agency to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Management Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Management Board in order to ensure continuity in its work. ***Due to the high market value of the skills required in the Agency's work, it is necessary to ensure that the salaries and the social conditions offered to all Agency staff are competitive and ensure that the best professionals can choose to work there.***

Justification

In order to have the appropriate level of expertise ENISA needs to be a competitive employer in a highly competitive market

Amendment 35

Proposal for a regulation

Recital 42

Text proposed by the Commission

(42) The smooth functioning of the Agency requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence. The Executive Director should prepare a proposal for the Agency's work programme, after prior consultation with the Commission, and take all necessary steps to ensure the proper execution of the work programme of the Agency. The Executive Director should prepare an annual report to be submitted to the Management Board, draw up a draft statement of estimates of revenue and expenditure for the Agency, and implement the budget. Furthermore, the Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific, technical, legal or socioeconomic nature. The Executive Director should ensure that the ad hoc Working Groups' members are selected according to the highest standards of expertise, taking due account of a representative balance, as appropriate according to the specific issues in question, between the public administrations of the Member States, the Union institutions and the private sector, including industry, users, and academic experts in network and information security.

Amendment 36

Proposal for a regulation

Recital 44

Amendment

(42) The smooth functioning of the Agency requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence. The Executive Director should prepare a proposal for the Agency's work programme, after prior consultation with the Commission, and take all necessary steps to ensure the proper execution of the work programme of the Agency. The Executive Director should prepare an annual report to be submitted to the Management Board, draw up a draft statement of estimates of revenue and expenditure for the Agency, and implement the budget. Furthermore, the Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific, technical, legal or socioeconomic nature. The Executive Director should ensure that the ad hoc Working Groups' members are selected according to the highest standards of expertise, taking due account of a representative **and gender** balance, as appropriate according to the specific issues in question, between the public administrations of the Member States, the Union institutions and the private sector, including industry, users, and academic experts in network and information security.

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 ***ENISA Advisory*** Group as an advisory body, to ensure regular dialogue with the private sector, consumers’ organisations, ***academia*** and other relevant stakeholders. The ***ENISA Advisory*** 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. ***Given the importance of certification requirements to ensure trust in IoT, the Commission will specifically consider implementing measures to ensure the pan-EU security standards harmonisation for IoT devices.***

Amendment 37

Proposal for a regulation
Recital 44 a (new)

Text proposed by the Commission

Amendment

(44 a) The Agency should have a Stakeholders Certification Group as an advisory body, to ensure regular dialogue with the private sector, consumers’ organisations, academia and other relevant stakeholders. The Stakeholders Certification Group, set up by the Executive Director, should be composed of a general advisory committee providing input on which ICT products and services to cover in future European IT security certification schemes, and ad-hoc committees providing inputs for the proposal, development and adoption of requested candidate European cybersecurity schemes.

Amendment 38

Proposal for a regulation Recital 46

Text proposed by the Commission

(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 39

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

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. ***An appropriate budget is paramount for ensuring that the Agency has sufficient capacities to fulfil all its growing tasks and objectives.*** 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, accountability, ***and the efficiency of the expenditure.***

Amendment

(47) Conformity assessment is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been

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

fulfilled. For the purposes of this Regulation, certification should be considered as a type of conformity assessment regarding the cybersecurity features of a product, process, service, system, or a combination of those ("ICT products, **processes** and services") by an independent third party **or, where permitted by self-assessment of** the product manufacturer or service provider. **Self-assessment may be undertaken by the product manufacturer, SMEs or service provider, specified in this Regulation and, if applicable, as provided by and in accordance with the New Legislative Framework. Moreover, it may be undertaken by the product manufacturer or operator where the likelihood of a cybersecurity incident occurring and/or the likelihood of such incident causing substantial harm to society or a large section thereof, is not expected to be high or substantial, taking into account the manufacturer or service provider's intended use of the product or service in question.** Certification cannot guarantee per se that **covered** ICT products, **processes** and services are cyber secure **and this must be duly communicated to consumers and businesses.** It is rather a procedure and technical methodology to attest that ICT products, **processes** and services have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example as specified in technical standards. **Those technical standards include an indication whether an ICT product, process and service is able to carry out its regular functions while being disconnected from the internet.**

Amendment 40

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, **processes** 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 41

Proposal for a regulation

Recital 49

Text proposed by the Commission

(49) In the 2016 Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", the Commission outlined the need for high-quality, affordable and interoperable cybersecurity products and solutions. The supply of ICT products and services within the single market remains very fragmented geographically. This is because the cybersecurity industry in Europe has developed largely on the basis of national governmental demand. In addition, the lack of interoperable solutions (technical standards), practices and EU-wide mechanisms of certification are among the other gaps affecting the single market in cybersecurity. On the one hand, this makes it difficult for European companies to compete at national, European and global level. On the other, it reduces the choice of viable and usable cybersecurity

Amendment

(49) In the 2016 Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", the Commission outlined the need for high-quality, affordable and interoperable cybersecurity products and solutions. The supply of ICT products, **processes** and services within the single market remains very fragmented geographically. This is because the cybersecurity industry in Europe has developed largely on the basis of national governmental demand. In addition, the lack of interoperable solutions (technical standards), practices and EU-wide mechanisms of certification are among the other gaps affecting the single market in cybersecurity. On the one hand, this makes it difficult for European companies to compete at national, European and global level. On the other, it reduces the choice of viable and usable

technologies that individuals and enterprises have access to. Similarly, in the Mid-Term Review on the implementation of the Digital Single Market Strategy, the Commission highlighted the need for safe connected products and systems, and indicated that the creation of a European ICT security framework setting rules on how to organise ICT security certification in the Union could both preserve trust in the internet and tackle the current fragmentation of the cybersecurity market.

cybersecurity technologies that individuals and enterprises have access to. Similarly, in the Mid-Term Review on the implementation of the Digital Single Market Strategy, the Commission highlighted the need for safe connected products and systems, and indicated that the creation of a European ICT security framework setting rules on how to organise ICT security certification in the Union could both preserve trust in the internet and tackle the current fragmentation of the cybersecurity market.

Amendment 42

Proposal for a regulation Recital 50

Text proposed by the Commission

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

Amendment

(50) Currently, the cybersecurity certification of ICT products, **processes** and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In this context, a certificate issued by one national cybersecurity authority is not in principle recognised by other Member States. Companies thus may have to certify their products, **processes** and services in several Member States where they operate, for example with a view to participating in national procurement procedures, **thereby adding to their costs**. 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, **risk-based** assurance **levels**, substantive criteria and actual utilisation. **Mutual recognition and trust among Member States is a key element in this respect. ENISA has an important role to play in helping the Member States develop a solid**

institutional structure and expertise in the protection against potential cyber-attacks. A case-by-case approach is required to ensure that services, processes and products are subject to appropriate certification schemes. Additionally, a risk-based approach is needed for the effective identification and mitigation of risks whilst acknowledging that a one size fits all scheme is not possible.

Amendment 43

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 EU's legitimate objectives in that regard.

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, ***processes*** 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, ***processes*** 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. ***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 the principle of 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 44

Proposal for a regulation Recital 52 a (new)

Text proposed by the Commission

Amendment

(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 45

Proposal for a regulation Recital 52 b (new)

Text proposed by the Commission

Amendment

(52b) Notes that certification schemes should build upon what already exists at national and international level, learning from current strong points and assessing and correcting weaknesses.

Amendment 46

Proposal for a regulation Recital 52 c (new)

Text proposed by the Commission

Amendment

(52c) Flexible cybersecurity solutions are necessary for the industry to stay ahead of malicious attacks and threats and therefore any certification scheme should avoid the risk of being outdated quickly.

Amendment 47

Proposal for a regulation Recital 53

Text proposed by the Commission

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

Amendment

(53) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products, ***processes*** and services. These schemes should be implemented and supervised by national certification supervisory authorities and certificates issued within these schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or other private organisations should fall outside the scope of the Regulation. However, the bodies operating such schemes may propose to the Commission to consider such schemes as a basis for approving them as a European scheme. ***The Agency should identify and assess the schemes already operated by the industry or private organisations in order to choose best practices which could become part of a European scheme. Industry actors can operate a self-assessment of their products or services prior to certification, thereby indicating their product or service is ready to begin the certification process if required or needed.***

Amendment 48

Proposal for a regulation Recital 53 a (new)

(53 a) *The Agency and the Commission should make the best use of already existing certification schemes on the EU and / or international level. ENISA should be able to assess which schemes already in use are fit for purpose and can be brought in the European legislation in cooperation with EU standardisation organisations and, as far as possible, internationally recognised. Existing good practices should be collected and shared among Member States.*

Amendment 49

Proposal for a regulation Recital 54

(54) The provisions of this Regulation should be without prejudice to Union legislation providing specific rules on certification of ICT products and services. In particular, the General Data Protection Regulation (GDPR) lays down provisions for the establishment of certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with that Regulation of processing operations by controllers and processors. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of relevant products and services. The present Regulation is without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR.

(54) The provisions of this Regulation should be without prejudice to Union legislation providing specific rules on certification of ICT products, ***processes*** and services. In particular, the General Data Protection Regulation (GDPR) lays down provisions for the establishment of certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with that Regulation of processing operations by controllers and processors. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of relevant products and services. The present Regulation is without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR.

Amendment 50

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 compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products **and** services. ICT products **and** services and related cybersecurity needs are so diverse that it is very difficult to come up with general cybersecurity requirements valid across the board. It is, therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, complemented by a set of specific cybersecurity objectives that need to be taken into account when designing European cybersecurity certification schemes. The modalities with which such objectives will be achieved in specific ICT products **and** services should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications.

Amendment

(55) The purpose of European cybersecurity certification schemes should be to ensure that ICT products, services **and processes** certified under such a scheme comply with specified requirements. Such requirements concern the ability to resist, at a given level of **risk**, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products, services **and processes**. ICT products, services **and processes** 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, services **and processes** 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. ***All actors involved in a given supply chain should be encouraged in order to develop and adopt security standards, technical norms and security by design principles, at all stages of the product, service or process lifecycle; each European cybersecurity certification scheme should be designed to reach this***

scope.

Amendment 51

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 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.

Amendment

(56) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products, ***processes*** or services ***on the basis of justified grounds namely existing national cybersecurity certification schemes fragmenting the internal market; a current or expected need to support Union law; or the opinion from the Member States' Certification Group or the Stakeholders' Certification Group.*** ***After assessing the candidate certification schemes*** proposed by ENISA ***on the basis of the Commission's request, the Commission*** should then be empowered to adopt the European cybersecurity certification ***schemes*** by means of ***delegated*** acts. Taking account of the general purpose and security objectives identified in this Regulation, ***those*** European cybersecurity certification schemes should specify a minimum set of elements concerning the subject-matter, the scope and functioning of the individual scheme. These should include among others the scope and object of the cybersecurity certification, including the categories of ICT products and services covered, the detailed specification of the cybersecurity requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods, as well as the intended level of assurance: basic, substantial and/or high.

Amendment 52

Proposal for a regulation
Recital 56 a (new)

Text proposed by the Commission

Amendment

(56 a) *The Agency should be the reference point of information about European cybersecurity schemes. It should maintain a website with all relevant information, including with regards to withdrawn and expired certificates and national certifications covered. The Agency should ensure that an adequate part of the content of its website is comprehensible for ordinary consumers.*

Amendment 53

Proposal for a regulation
Recital 56 b (new)

Text proposed by the Commission

Amendment

(56 b) *Defining assurance levels for certificates is necessary in order to give an indication to the end user of the expected type of cyber threats that the cybersecurity measures within the product, process or service intend to prevent. Cyber threats must be defined taking into account the expected risk and the capabilities of the author or authors of the attack in the context of the expected use of the ICT product, process or service covered. Assurance level ‘basic’ refers to the capacity to resist attacks that can be avoided with basic cybersecurity measures of and that can be checked easily by reviewing the technical documentation. Assurance level ‘substantial’ refers to the capacity to resist known types of attacks by an attacker with a certain level of sophistication but with limited resources. Assurance level ‘high’ refers to the capacity to resist unknown vulnerabilities and sophisticated attacks with state-of-the-art techniques and significant*

resources such as funded multidisciplinary teams.

Amendment 54

Proposal for a regulation Recital 56 c (new)

Text proposed by the Commission

Amendment

(56 c) In order to avoid fragmentation of the internal market due to national cybersecurity schemes, support future legislations and increase trust and security, 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 the setting of the priorities for European cybersecurity certification, the adoption of the rolling programme and the adoption of European certification schemes. 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 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 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 55

Proposal for a regulation Recital 56 d (new)

Text proposed by the Commission

Amendment

(56d) 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 56

Proposal for a regulation

Recital 57

Text proposed by the Commission

(57) Recourse to European cybersecurity certification should remain voluntary, unless otherwise provided in Union or national legislation. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the **implementing** act. Moreover, Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme.

Amendment

(57) Recourse to European cybersecurity certification should remain voluntary, unless otherwise provided in Union or national legislation. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products, **processes** and services covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the **delegated** act. Moreover, Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme. **However, this Regulation should be without prejudice to national schemes that Member States remain sovereign to manage for ICT products, processes and services used for their sovereign domain needs.**

Amendment 57

Proposal for a regulation Recital 57 a (new)

Text proposed by the Commission

Amendment

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

Amendment 58

Proposal for a regulation Recital 57 b (new)

Text proposed by the Commission

Amendment

(57b) When proposing new European cybersecurity schemes, ENISA and other relevant bodies should pay due attention to the competitive dynamics of the proposal, specifically making sure that where the sector concerned has many of small and medium sized enterprises, such as in software development, certification schemes do not form a barrier for entry for new businesses and innovations.

Amendment 59

Proposal for a regulation Recital 57 c (new)

Text proposed by the Commission

Amendment

(57c) European cybersecurity schemes will help to harmonise and unify cybersecurity practices within the Union. They must not however become the minimum level of cybersecurity. The design of European cybersecurity schemes should also take into account and allow for development of new

innovations in the field of cybersecurity.

Amendment 60

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.

Amendment

(58) Once a European cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT ***processes or*** services should be able to submit an application for certification of their products or services to a conformity assessment body of their choice ***anywhere in the Union***. Conformity assessment bodies should be accredited by an accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements. Accreditation bodies should revoke an accreditation of a conformity assessment body where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation. ***Audits by the Agency should be carried out to ensure an equivalent level of quality and diligence of conformity assessment bodies with a view to avoiding regulatory arbitrage. The results should be reported to the Agency, the Commission and Parliament and should be made publicly available.***

Amendment 61

Proposal for a regulation

Recital 58 a (new)

Text proposed by the Commission

Amendment

(58 a) ***The mandatory use of***

European cybersecurity certification should be restricted to cases where risk analysis justifies the cost to industry, citizens and consumers. Incidents disrupting essential services can impede the pursuit of economic activities, generate substantial financial loss, undermine user confidence and cause major damage to the economy of the Union. The mandatory use of European cybersecurity certification by operators of essential services should be restricted to those elements that are critical for their functioning and should not be extensive to general-purpose products, processes and services, which would create an unjustified cost for the industry and the consumers. The Commission should work together with the Cooperation Group set up pursuant to Article 11 of Directive (EU) 2016/1148 to define a list of categories of products, processes and services that are specifically intended for the use by operators of essential services and whose malfunctioning in the event of an incident could have a significant disruptive effect on the essential service. That list should be compiled progressively and should be updated when necessary. Only products, processes and services on that list should be mandatory for the operators of essential requirements.

Amendment 62

Proposal for a regulation Recital 58 b (new)

Text proposed by the Commission

Amendment

(58 b) *The presence of cross references in national legislation that refer to a national standard which has ceased to produce legal effects due to the entry into force of a European Certification scheme can be a potential source of confusion for manufacturers and end users. In order to avoid that*

manufacturers continue to implement specifications corresponding to national certificates that are no longer in force, Member States should, in accordance with its obligations under the Treaties, adapt their national legislation to reflect the adoption of an European Certification scheme.

Amendment 63

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 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.

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, ***and to ensure that the European cybersecurity certificates are recognised on their territory.*** 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, ***or in relation to alleged failures to recognise certificates on their territory,*** 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, ***processes*** and services with the requirements of this Regulation or specific cybersecurity schemes, ***or the non-recognition of European cybersecurity***

certificates. 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 in accordance 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 64

Proposal for a regulation

Recital 60

Text proposed by the Commission

(60) With a view to ensuring the consistent application of the European cybersecurity certification framework, a **European Cybersecurity Certification Group (the 'Group')** consisting of national certification supervisory authorities should be established. The main tasks of the Group should be to advise and assist the Commission in its work to ensure a consistent implementation and application of the European cybersecurity certification

Amendment

(60) With a view to ensuring the consistent application of the European cybersecurity certification framework, a **Member States Certification Group** consisting of national certification supervisory authorities should be established. The main tasks of the **Member States Certification Group** should be to advise and assist the Commission in its work to ensure a consistent implementation and application of the European

framework; to assist and closely cooperate with the Agency in the preparation of candidate cybersecurity certification schemes; recommend that the Commission request the Agency to prepare a candidate European cybersecurity certification scheme; and to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

cybersecurity certification framework; to assist and closely cooperate with the Agency in the preparation of candidate cybersecurity certification schemes; recommend that the Commission request the Agency to prepare a candidate European cybersecurity certification scheme; and to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

Amendment 65

Proposal for a regulation Recital 60 a (new)

Text proposed by the Commission

Amendment

(60 a) In order to ensure the equivalence of the level of competence of conformity assessment bodies, to facilitate mutual recognition and to promote the overall acceptance of certificates and conformity assessment results issued by conformity assessment bodies, it is necessary that national certification supervisory authorities operate a rigorous and transparent peer evaluation system and regularly undergo such evaluation.

Amendment 66

Proposal for a regulation Recital 60 b (new)

Text proposed by the Commission

Amendment

(60 b) Effective cooperation among national certification supervisory authorities is essential for the proper implementation of peer evaluation and with regard to cross-border accreditation. In the interests of transparency it is, therefore, necessary to provide for an obligation for national certification

supervisory authorities to exchange information among themselves and to provide the national authorities and the Commission with relevant information. Updated and accurate information concerning the availability of accreditation activities operated by national accreditation bodies should also be made public and, therefore, accessible in particular to conformity assessment bodies.

Amendment 67

Proposal for a regulation Recital 61

Text proposed by the Commission

(61) In order to raise awareness and facilitate the acceptance of future EU cyber security schemes, the European Commission may issue general or sector-specific cyber security guidelines, e.g. on good cyber security practices or responsible cyber security behaviour highlighting the positive effect of the use of certified ICT products and services.

Amendment

(61) In order to raise awareness and facilitate the acceptance of future EU cyber security schemes, the European Commission may issue general or sector-specific cyber security guidelines, e.g. on good cyber security practices or responsible cyber security behaviour highlighting the positive effect of the use of certified ICT products, **processes** and services.

Amendment 68

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

Amendment

(63) In order to specify further the criteria for the accreditation of conformity assessment bodies, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. The Commission should carry out appropriate consultations during its preparatory work, including at expert level **and with relevant stakeholders, as**

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.

appropriate. 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 69

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) ***Delegated acts could be furthermore adopted*** on European cybersecurity certification schemes for ICT products, ***processes*** 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 70

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,***

Amendment

(66) The Agency's operations should be evaluated ***continuously and*** independently. The evaluation should have regard to the Agency achieving its objectives, its working practices and the relevance of its tasks, ***in particular its coordinating role***

effectiveness and efficiency of the European cybersecurity certification framework.

vis-à-vis the Member States and their national authorities. In case of a review, the Commission should evaluate the possibility of the Agency to act as a one-stop-shop for Member States and Union institutions and bodies.

Amendment 71

Proposal for a regulation Recital 66 a (new)

Text proposed by the Commission

Amendment

(66 a) *The evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework. In the case of a review the Commission could evaluate a role for the Agency to assess third country products and services entering the Union market and the possibility to blacklist companies that do not comply with Union rules.*

Amendment 72

Proposal for a regulation Recital 66 b (new)

Text proposed by the Commission

Amendment

(66 b) *The evaluation should analyse the level of cybersecurity of products and services sold in the Union. In the case of a review, the Commission should evaluate whether to include cybersecurity essential requirements as a condition for access to the internal market.*

Amendment 73

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

Text proposed by the Commission

(a) lays down the objectives, tasks and organisational aspects of *ENISA*, the "*EU Cybersecurity Agency*", hereinafter 'the Agency'; and

Amendment

(a) lays down the objectives, tasks and organisational aspects of the '*European Union Agency for Network and Information Security*' ('the Agency'); and

Amendment 74

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

Text proposed by the Commission

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

Amendment

(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of *avoiding a fragmentation of certification schemes in the Union and* ensuring an adequate level of cybersecurity of ICT products, *processes* and services in the Union *which applies* without prejudice to specific provisions regarding voluntary *and, where appropriate,* mandatory certification *where provided for in this Regulation or* in other Union acts.

Amendment 75

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

Text proposed by the Commission

Amendment

The Agency shall carry out its tasks without prejudice to the Member States' competences regarding cybersecurity, and in particular, to the Member States' competences concerning public security, defence, national security and criminal law.

Amendment 76

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

Text proposed by the Commission

(1) ‘cybersecurity’ **comprises** all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;

Amendment

(1) ‘cybersecurity’ **means** all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;

Amendment 77

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

Text proposed by the Commission

(2) ‘network and information system’ means a system **within the meaning of** point (1) of Article 4 of Directive (EU) 2016/1148;

Amendment

(2) ‘network and information system’ means a **network and information** system **as defined in** point (1) of Article 4 of Directive (EU) 2016/1148;

Amendment 78

Proposal for a regulation
Article 2 – paragraph 1 – point 3

Text proposed by the Commission

(3) ‘national strategy on the security of network and information systems’ means a **framework within the meaning of** point (3) of Article 4 of Directive (EU) 2016/1148;

Amendment

(3) ‘national strategy on the security of network and information systems’ means a **national strategy on the security of network and information systems as defined in** point (3) of Article 4 of Directive (EU) 2016/1148;

Amendment 79

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

Text proposed by the Commission

(4) ‘operator of essential services’ means a **public or private entity** as defined in point (4) of Article 4 of Directive (EU)

Amendment

(4) ‘operator of essential services’ means an **operator of essential services** as defined in point (4) of Article 4 of Directive (EU)

2016/1148;

2016/1148;

Amendment 80

Proposal for a regulation

Article 2 – paragraph 1 – point 5

Text proposed by the Commission

(5) ‘digital service provider’ means **any legal person that provides a** digital service as defined in point (6) of Article 4 of Directive (EU) 2016/1148

Amendment

(5) ‘digital service provider’ means a digital service **provider** as defined in point (6) of Article 4 of Directive (EU) 2016/1148

Amendment 81

Proposal for a regulation

Article 2 – paragraph 1 – point 6

Text proposed by the Commission

(6) ‘incident’ means **any event** as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

Amendment

(6) ‘incident’ means an **incident** as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

Amendment 82

Proposal for a regulation

Article 2 – paragraph 1 – point 7

Text proposed by the Commission

(7) ‘incident handling’ means **any procedure** as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

Amendment

(7) ‘incident handling’ means **incident handling** as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

Amendment 83

Proposal for a regulation

Article 2 – paragraph 1 – point 8

Text proposed by the Commission

(8) ‘cyber threat’ means any potential circumstance **or** event that may adversely

Amendment

(8) ‘cyber threat’ means any potential circumstance, event **or any intentional**

impact network and information systems, their users and affected persons.

action, including an automated command, that may **damage, disrupt or otherwise** adversely impact network and information systems, their users and affected persons.

Amendment 84

Proposal for a regulation Article 2 – paragraph 1 – point 8 a (new)

Text proposed by the Commission

Amendment

(8 a) ‘cyber hygiene’ means simple routine measures that when implemented and carried out regularly by users and businesses online minimise their exposure to risks from cyber threats.

Amendment 85

Proposal for a regulation Article 2 – paragraph 1 – point 9

Text proposed by the Commission

Amendment

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

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

Amendment 86

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

Text proposed by the Commission

Amendment

(10) ‘European cybersecurity certificate’ means a document issued by a conformity

(10) ‘European cybersecurity certificate’ means a document issued by a conformity

assessment body attesting that a given ICT product or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;

assessment body attesting that a given ICT product, or service *or process* fulfils the specific requirements laid down in a European cybersecurity certification scheme;

Amendment 87

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

Text proposed by the Commission

Amendment

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

Amendment 88

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

Text proposed by the Commission

Amendment

(11 b) ‘consumer electronic device’ means devices consisting of hardware and software that process personal data or connect to the Internet for the operation of domotics and home control appliances, office appliances, routing equipment and devices that connect to a network, such as smart TVs, toys and gaming consoles, virtual or personal assistants, connected streaming devices, wearables, voice-command and virtual reality systems;

Amendment 89

Proposal for a regulation Article 2 – paragraph 1 – point 16

Text proposed by the Commission

Amendment

(16) ‘standard’ means a standard as defined in point (1) of Article 2 of

(16) ‘standard , *technical specification and ICT technical specification*’ means a

Regulation (EU) No 1025/2012.

standard, ***technical specification or ICT technical specification*** as defined in point (1), (4) and (5) of Article 2 of Regulation (EU) No 1025/2012;

Amendment 90

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

Text proposed by the Commission

Amendment

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

Amendment 91

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

Text proposed by the Commission

Amendment

(16 b) ‘self-assessment’ means the statement of conformity by which the manufacturer declares that specific requirements set in a certification scheme relating to products, processes and services have been fulfilled;

Amendment 92

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

Text proposed by the Commission

Amendment

(16 c) ‘security by default’ means a situation where if a product, software or process can be set up in a way that ensures a higher degree of security, the first user should receive the default configuration with the most secure settings possible. If, on a case by case

basis, a risk and usability analysis leads to the conclusion that such a setting is not feasible, users should be prompted to opt for the most secure setting.

Amendment 93

Proposal for a regulation

Article 2 – paragraph 1 – point 16 d (new)

Text proposed by the Commission

Amendment

(16 d) ‘operators of essential services’ means operators of essential services as defined in point (4) of Article 4 of Directive(EU) 2016/1148.

Amendment 94

Proposal for a regulation

Article 3 – paragraph 1

Text proposed by the Commission

Amendment

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

1. The Agency shall undertake the tasks assigned to it by this Regulation ***and shall be reinforced*** 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; and to ensure consistency by taking into account the Member States’ cooperation achievements under the NIS Directive.***

Amendment 95

Proposal for a regulation

Article 4 – paragraph 1

Text proposed by the Commission

Amendment

1. The Agency shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical

1. The Agency shall be a centre of ***theoretical and practical*** expertise on cybersecurity by virtue of its

quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks.

independence, the scientific and technical quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks.

Amendment 96

Proposal for a regulation Article 4 – paragraph 2

Text proposed by the Commission

2. The Agency shall assist the Union institutions, agencies and bodies, as well as Member States, in developing and implementing policies related to cybersecurity.

Amendment

2. The Agency shall assist the Union institutions, agencies and bodies, as well as Member States, in developing and implementing policies related to cybersecurity ***and raising awareness among citizens and businesses.***

Amendment 97

Proposal for a regulation Article 4 – paragraph 3

Text proposed by the Commission

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

Amendment

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

Amendment 98

Proposal for a regulation Article 4 – paragraph 4

Text proposed by the Commission

4. The Agency shall promote cooperation **and** coordination at Union level among Member States, Union institutions, agencies and bodies, and relevant stakeholders, **including the private sector**, on matters related to cybersecurity.

Amendment

4. The Agency shall promote cooperation, coordination **and information sharing** at Union level among Member States, Union institutions, agencies and bodies, and relevant stakeholders, on matters related to cybersecurity.

Amendment 99

Proposal for a regulation
Article 4 – paragraph 5

Text proposed by the Commission

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

Amendment

5. The Agency shall **contribute to increasing** cybersecurity capabilities at Union level in order to complement the action of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents **and in order to carry out its task of assisting Union institutions in developing policies related to cybersecurity**.

Amendment 100

Proposal for a regulation
Article 4 – paragraph 6

Text proposed by the Commission

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

Amendment

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

market, *as well as increasing the compatibility between existing national and international certification schemes*

Amendment 101

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 ***and support projects contributing to*** a high level of awareness, ***cyber hygiene and cyber literacy among*** citizens and businesses on issues related to the cybersecurity.

Amendment 102

Proposal for a regulation Article 5 – paragraph 1

Text proposed by the Commission

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

Amendment

1. assisting and advising, in particular by providing its independent opinion ***and analysis of relevant activities in cyberspace*** and 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;

Amendment 103

Proposal for a regulation Article 5 – paragraph 2

Text proposed by the Commission

2. assisting Member States to implement consistently the Union policy and law regarding cybersecurity notably in relation to Directive (EU) 2016/1148,

Amendment

2. assisting Member States to implement consistently the Union policy and law regarding cybersecurity notably in relation to Directive (EU) 2016/1148,

including by means of opinions, guidelines, advice and best practices on topics such as risk management, incident reporting and information sharing, as well as facilitating the exchange of best practices between competent authorities in this regard;

Directive ... establishing the European Electronic Communications Code, Regulation (EU) 2016/679 and Directive 2002/58/EC including by means of opinions, guidelines, advice and best practices on topics such as ***secure software and systems development***, risk management, incident reporting and information sharing, ***technical and organisational measures, in particular the establishment of coordinated vulnerability disclosure programmes*** as well as facilitating the exchange of best practices between competent authorities in this regard;

Amendment 104

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

Text proposed by the Commission

Amendment

2 a. the development and promotion of policies that would sustain the general availability or integrity of the public core of the open internet, which provide the essential functionality to the Internet as a whole and which underpin its normal operation, including, but not limited to, the security and stability of key protocols (in particular DNS, BGP, and IPv6), the operation of the Domain Name System (including those of all Top Level Domains), and the operation of the Root Zone.

Amendment 105

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

Text proposed by the Commission

Amendment

(2) the promotion of an enhanced level of security of electronic communications, including by providing expertise and

(2) the promotion of an enhanced level of security of electronic communications, ***data storage and data processing***,

advice, as well as facilitating the exchange of best practices between competent authorities;

including by providing expertise and advice, as well as facilitating the exchange of best practices between competent authorities;

Amendment 106

Proposal for a regulation Article 5 – paragraph 5 a (new)

Text proposed by the Commission

Amendment

5 a. assisting Member States to implement the Union policy and law relating to data protection consistently, in particular Regulation (EU) 2016/679, as well as assisting the European Data Protection Board (EDPB) for the development of guidelines related to the implementation of Regulation (EU) 2016/679 for cybersecurity purposes. The EDPB shall consult the Agency every time it issues an opinion or a decision concerning the implementation of GDPR and cybersecurity, non-exhaustively on issues related to privacy impact assessments, data breach notification, security processing, security requirements, and privacy by design.

Amendment 107

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

Text proposed by the Commission

Amendment

(a a) Members States and Union institutions in establishing and implementing coordinated vulnerability disclosure policies and government vulnerability disclosure review processes, whose practices and determinations should be transparent and subject to independent oversight.

Amendment 108

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

Text proposed by the Commission

Amendment

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

Amendment 109

Proposal for a regulation Article 6 – paragraph 1 – point g

Text proposed by the Commission

Amendment

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

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

Amendment 110

Proposal for a regulation Article 6 – paragraph 2

Text proposed by the Commission

Amendment

2. The Agency shall facilitate the establishment of and continuously support sectoral Information Sharing and Analysis Centres (ISACs), in particular in the sectors listed in Annex II of Directive (EU) 2016/1148, by providing best practices and

2. The Agency shall facilitate the establishment of and continuously support sectoral Information Sharing and Analysis Centres (ISACs), in particular in the sectors listed in Annex II of Directive (EU) 2016/1148, by providing best practices and

guidance on available tools, procedure, as well as on how to address regulatory issues related to information sharing.

guidance on available tools, procedure, ***cyber hygiene principles*** as well as on how to address regulatory issues related to information sharing.

Amendment 111

Proposal for a regulation Article 7 – paragraph 1

Text proposed by the Commission

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

Amendment

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

Amendment 112

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

Text proposed by the Commission

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

Amendment

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

Amendment 113

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

Text proposed by the Commission

Amendment

(b a) where a situation requires urgent action when an incident has a significant

disruptive effect, a Member State may request the assistance of experts from the Agency to assess the situation. The request shall include a description of the situation, the possible aims and envisaged needs.

Amendment 114

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 *assistance either in the form of advice for the prevention of future incidents, or in the form of assisting in the response to current large scale* 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 perform the above activities by receiving relevant information from the affected Member States and by utilising its own resources on threat analysis as well as resources on incident response.* 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 *one Member State. In so doing, the Agency shall make sure not to disclose the actions taken by Member States to safeguard their essential State functions, in particular those concerning national security.*

Amendment 115

Proposal for a regulation Article 7 – paragraph 6

Text proposed by the Commission

6. The Agency shall organise annual cybersecurity exercises at Union level, and support Member States and EU institutions, agencies and bodies in organising exercises following their request(s). Annual exercises at Union level shall include technical, operational and strategic elements and help to prepare the cooperative response at the Union level to large-scale cross-border cybersecurity incidents. The Agency shall also contribute to and help organise, where appropriate, sectoral cybersecurity exercises together with relevant ISACs and permit ISACs to participate also to Union level cybersecurity exercises.

Amendment

6. The Agency shall organise **regular, and in any event at least** annual cybersecurity exercises at Union level, and support Member States and EU institutions, agencies and bodies in organising exercises following their request(s). Annual exercises at Union level shall include technical, operational and strategic elements and help to prepare the cooperative response at the Union level to large-scale cross-border cybersecurity incidents. The Agency shall also contribute to and help organise, where appropriate, sectoral cybersecurity exercises together with relevant ISACs and permit ISACs to participate also to Union level cybersecurity exercises.

Amendment 116

Proposal for a regulation
Article 7 – paragraph 7

Text proposed by the Commission

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

Amendment

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

Amendment 117

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

Text proposed by the Commission

Amendment

7 a. The Agency shall, where appropriate and subject to prior approval by the Commission, contribute to cyber cooperation with the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy.

Amendment 118

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

Text proposed by the Commission

Amendment

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

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

Amendment 119

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

Text proposed by the Commission

Amendment

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

(c) supporting the technical handling of an incident or crisis, **based on its own independent expertise and resources**, including facilitating the **voluntary** sharing of technical solutions between Member States;

Amendment 120

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

Text proposed by the Commission

Amendment

8 a. The Agency shall arrange for an exchange of views when needed and shall

assist Member States' authorities in the coordination of their response, in accordance with the principles of subsidiarity and proportionality.

Amendment 121

Proposal for a regulation Article 7 a (new)

Text proposed by the Commission

Amendment

Article 7 a

Technical capabilities of the Agency

1. For the purpose of meeting the objectives described in Article 7, and in accordance with the working programme of the Agency, the Agency shall, inter alia, develop the following technical capabilities and skills:

(a) the ability to collect information on cybersecurity threats from open source; and

(b) the ability to deploy technical equipment, tools and expertise remotely.

2. For the purpose of meeting the technical capabilities referred to in paragraph 1 of this Article and of developing the relevant skills, the Agency shall:

(a) ensure that its recruitment processes reflect the diverse technical skills required; and

(b) cooperate with CERT EU and Europol in accordance with Article 7, paragraph 2 of this Regulation.

Amendment 122

Proposal for a regulation Article 8 – paragraph 1 – point a – introductory part

Text proposed by the Commission

Amendment

(a) support and promote the development and implementation of the Union policy on cybersecurity certification of ICT products **and** services, as established in Title III of this Regulation, by:

(a) support and promote the development and implementation of the Union policy on cybersecurity certification of ICT products services, **and processes** as established in Title III of this Regulation, by:

Amendment 123

Proposal for a regulation

Article 8 – paragraph 1 – point a – point -1 (new)

Text proposed by the Commission

Amendment

(-1) on an ongoing basis identifying standards, technical specifications and ICT technical specifications;

Amendment 124

Proposal for a regulation

Article 8 – paragraph 1 – point a – point 1

Text proposed by the Commission

Amendment

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

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

Amendment 125

Proposal for a regulation

Article 8 – paragraph 1 – point a – point 1 a (new)

Text proposed by the Commission

Amendment

(1 a) carrying out, in cooperation with the Member States Certification Group

pursuant to Article 53 of this Regulation, assessments of the procedures for issuing European cybersecurity certificates put in place by conformity assessment bodies referred to in Article 51 of this Regulation, with a view to ensuring the uniform application of this Regulation by conformity assessment bodies when issuing certificates;

Amendment 126

Proposal for a regulation

Article 8 – paragraph 1 – point a – point 1 b (new)

Text proposed by the Commission

Amendment

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

Amendment 127

Proposal for a regulation

Article 8 – paragraph 1 – point a – point 2

Text proposed by the Commission

Amendment

(2) assisting the Commission in providing the secretariat to the **European Cybersecurity** Certification Group pursuant to Article 53 of this Regulation;

(2) assisting the Commission in providing the secretariat to the **Member States** Certification Group pursuant to Article 53 of this Regulation;

Amendment 128

Proposal for a regulation

Article 8 – paragraph 1 – point a – point 3

Text proposed by the Commission

Amendment

(3) compiling and publishing guidelines and developing good practices concerning the cybersecurity requirements of ICT products and services, in cooperation with

(3) compiling and publishing guidelines and developing good practices, **including on cyber hygiene principles** concerning the cybersecurity requirements of ICT

national certification supervisory authorities and the industry;

products, **processes** and services, in cooperation with national certification supervisory authorities and the industry **in a formal, standardised and transparent process**;

Amendment 129

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

Text proposed by the Commission

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

Amendment

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

Amendment 130

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

Text proposed by the Commission

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

Amendment

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

Amendment 131

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

Amendment 132

Proposal for a regulation

Article 9 – paragraph 1 – point g

Text proposed by the Commission

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

Amendment

(g) organise, in cooperation with the Member States and Union institutions, bodies, offices and agencies regular ***communication*** campaigns to ***encourage a broad public debate;***

Amendment 133

Proposal for a regulation

Article 9 – paragraph 1 – point g a (new)

Text proposed by the Commission

Amendment

(g a) support closer coordination and exchange of best practices among Member States on cybersecurity education and literacy, cyber hygiene and raising awareness.

Amendment 134

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 **areas** of cybersecurity, **data protection and privacy**, 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 135

Proposal for a regulation

Article 10 – paragraph 1 – point b a (new)

Text proposed by the Commission

Amendment

(b a) commission its own research activities in areas of interest that are not yet covered by existing Union research programmes, where there is a clearly identified European added value.

Amendment 136

Proposal for a regulation

Article 11 – paragraph 1 – point c a (new)

Text proposed by the Commission

Amendment

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

Amendment 137

Proposal for a regulation

Article 12 – paragraph 1 – point d

Text proposed by the Commission

(d) a **Permanent Stakeholders’** Group which shall exercise the functions set out in Article 20.

Amendment

(d) an **ENISA Advisory** Group which shall exercise the functions set out in Article 20.

Amendment 138

Proposal for a regulation

Article 14 – paragraph 1 – point e

Text proposed by the Commission

(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

(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, describe **the effectiveness of the expenditure and assess** how **efficient** the Agency has **been and to what extent it has** met its performance indicators. The annual report shall be made public;

Amendment 139

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 140

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 141

Proposal for a regulation Article 16 – paragraph 4

Text proposed by the Commission

4. Members of the **Permanent Stakeholder** Group may take part, upon invitation from the Chairperson, in the meetings of the Management Board, without voting rights.

Amendment

4. Members of the **ENISA Advisory** Group may take part, upon invitation from the Chairperson, in the meetings of the Management Board, without voting rights.

Amendment 142

Proposal for a regulation Article 18 – paragraph 3

Text proposed by the Commission

3. The Executive Board shall be composed of five members appointed from among the members of the Management Board amongst whom the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission. The Executive Director shall take part in the meetings of the Executive Board, but shall not have the right to vote.

Amendment

3. The Executive Board shall be composed of five members appointed from among the members of the Management Board amongst whom the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission. The Executive Director shall take part in the meetings of the Executive Board, but shall not have the right to vote. **The appointments shall aim to achieve a balanced representation of genders on the**

Executive Board.

Justification

The Executive Board appointments need to also aim for gender balance, mirroring the provisions for the Management Board in art. 13 point 3.

Amendment 143

Proposal for a regulation Article 19 – paragraph 2

Text proposed by the Commission

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

2. The Executive Director shall report ***annually*** to the European Parliament on the performance of his or her duties ***or*** when invited to do so. The Council may invite the Executive Director to report on the performance of his or her duties.

Amendment 144

Proposal for a regulation Article 19 – paragraph 5 a (new)

Text proposed by the Commission

Amendment

5a. The Executive Director shall also be entitled to act as an institutional special adviser on cybersecurity policy to the President of the European Commission, with a mandate defined in Commission Decision C(2014) 541 of 6 February 2014.

Amendment 145

Proposal for a regulation Article 20 – title

Text proposed by the Commission

Amendment

Permanent Stakeholders' Group

ENISA Advisory Group

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

Amendment 146

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, **in the transparent manner**, shall set up an **ENISA Advisory** Group composed of recognised **security** experts representing the relevant stakeholders, such as the ICT industry – **including SMEs, operators of essential services according to the NIS Directive**, providers of electronic communications networks or services available to the public, consumer groups, academic experts in the cybersecurity, **European Standards Organisations (ESOs), EU agencies** 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. **The Management Board shall ensure an appropriate balance between different stakeholder groups.**

Amendment 147

Proposal for a regulation Article 20 – paragraph 2

Text proposed by the Commission

2. Procedures for the **Permanent Stakeholders’** Group, in particular regarding the number, composition, and the appointment of its members by the Management Board, the proposal by the Executive Director and the operation of the Group, shall be specified in the Agency’s internal rules of operation and shall be made public.

Amendment

2. Procedures for the **ENISA Advisory** Group, in particular regarding the number, composition, and the appointment of its members by the Management Board, the proposal by the Executive Director and the operation of the Group, shall be specified in the Agency’s internal rules of operation and shall be made public.

Amendment 148

Proposal for a regulation Article 20 – paragraph 3

Text proposed by the Commission

3. ***The Permanent Stakeholders'*** Group shall be chaired by the Executive Director or by any person the Executive Director appoints on a case-by-case basis.

Amendment

3. ***The ENISA Advisory*** Group shall be chaired by the Executive Director or by any person the Executive Director appoints on a case-by-case basis.

Amendment 149

Proposal for a regulation Article 20 – paragraph 4

Text proposed by the Commission

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

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

Amendment 150

Proposal for a regulation Article 20 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4 a. The ENISA Advisory Group will provide regular updates on its planning

throughout the year and set out the objectives in its work programme which shall be published every six months to ensure transparency;

Amendment 151

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 **ENISA Advisory** Group shall advise the Agency in respect of the performance of its activities, **except of the application of the title III of this Regulation**. 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 issues related to the work programme.

Amendment 152

Proposal for a regulation Article 20 a (new)

Text proposed by the Commission

Amendment

Article 20 a

Stakeholder Certification Group

1. **The Executive Director shall setup a Stakeholder Certification Group, composed of a general advisory committee providing general advice on the application of the title III of this Regulation and shall setup ad-hoc committees for the proposal, development and adoption of each candidate scheme. Members of this Group shall be selected among recognised security experts representing relevant stakeholders, such as the ICT industry - including SMEs, operators of essential services according**

to the NIS Directive, providers of electronic communications networks or services available to the public, , consumer groups, academic experts in the cybersecurity and European Standards Organisations (ESOs) 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.

2. Procedures for the Stakeholder Certification Group, in particular regarding the number, composition, and the appointment of its members by the Executive Director, shall be specified in the Agency's internal rules of operation, follow best practices in ensuring a fair representation and equal rights for all stakeholders and shall be made public.

3. Members of the Management Board may not be members of the Stakeholder Certification Group. Members of the ENISA Advisory Group may also be Members of the Stakeholder Certification Group. Experts from the Commission and the Member States shall be entitled, upon invitation, to be present at the meetings of the Stakeholder Certification Group. Representatives of other bodies deemed relevantly the Executive Director, may be invited to attend the meetings of the Stakeholder Certification Group and to participate in its work.

4. The Stakeholder Certification Group shall advise the Agency in respect of the performance of its activities with regards Title III of this Regulation. It shall in particular be entitled to propose to the Commission the preparation of a candidate European cybersecurity certification scheme, as provided in Article 44 of this Regulation, as well as to participate to the procedures referred to in Articles 43 to 48 and Article 53 of this Regulation for the approval of such schemes.

Amendment 153

Proposal for a regulation Article 21 a (new)

Text proposed by the Commission

Amendment

Article 21 a

Request to the Agency

- 1. The Agency should establish and manage a single entry point through which requests for advice and assistance falling within the Agency's objectives and tasks shall be addressed. These requests should be accompanied by background information explaining the issue to be addressed. Agency should draw up the potential resource implications, and, in due course, follow-up to the requests. If the Agency refuses a request, it shall give a justification.*
- 2. Requests referred to in paragraph 1 may be made by:*
 - a) the European Parliament;*
 - b) the Council;*
 - c) the Commission; and*
 - d) any competent body appointed by a Member State, such as a national regulatory authority as defined in Article 2 of Directive 2002/21/EC.*
- 3. The practical arrangements for applying paragraphs 1 and 2, regarding in particular submission, prioritisation, follow-up and information, shall be laid down by the Management Board in the Agency's internal rules of operation.*

Amendment 154

Proposal for a regulation Article 24 – paragraph 2

Text proposed by the Commission

Amendment

2. Members of the Management Board,

2. Members of the Management Board,

the Executive Director, the members of the **Permanent Stakeholders** Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union (TFEU), even after their duties have ceased.

the Executive Director, the members of the **ENISA Advisory** Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union (TFEU), even after their duties have ceased.

Amendment 155

Proposal for a regulation

Article 26 – paragraph 1 – subparagraph 1 a (new)

Text proposed by the Commission

Amendment

The provisional draft statement of estimates shall be based on the objectives and expected results of the single programming document referred to in Article 21, paragraph 1 of this Regulation and shall take into account the financial resources necessary to achieve those objectives and expected results, in accordance with the principle of performance-based budgeting.

Amendment 156

Proposal for a regulation

Article 30 – paragraph 2

Text proposed by the Commission

Amendment

2. The Court of Auditors shall have the power of audit, on the basis of documents and on the spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds from the Agency.

2. The Court of Auditors shall have the power of audit, on the basis of documents and on the spot ***inspections***, over all grant beneficiaries, contractors and subcontractors who have received Union funds from the Agency.

Amendment 157

Proposal for a regulation
Article 36 – paragraph 5

Text proposed by the Commission

5. The personal liability of its servants towards the Agency shall be governed by the relevant conditions applying to the staff of the Agency.

Amendment

5. The personal liability of its servants towards the Agency shall be governed by the relevant conditions applying to the staff of the Agency. ***Effective recruitment of staff shall be ensured.***

Amendment 158

Proposal for a regulation
Article 37 – paragraph 2

Text proposed by the Commission

2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union.

Amendment

2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union ***or other translation services providers in accordance with the procurement rules and within the limits established by the relevant financial rules.***

Amendment 159

Proposal for a regulation
Article 39 – paragraph 1

Text proposed by the Commission

1. In so far as is necessary in order to achieve the objectives set out in this Regulation, the Agency may cooperate with the competent authorities of third countries or with international organisations or both. To this end, the Agency may, subject to prior approval by the Commission, establish working arrangements with the authorities of third countries and international organisations. These arrangements shall not create legal obligations incumbent on the Union and its Member States.

Amendment

1. In so far as is necessary in order to achieve the objectives set out in this Regulation, the Agency may cooperate with the competent authorities of third countries or with international organisations or both. To this end, the Agency may, subject to prior approval by the Commission, establish working arrangements with the authorities of third countries and international organisations. ***Cooperation with NATO, where it takes place, may include joint cybersecurity exercises and joint cyber incident***

response coordination. These arrangements shall not create legal obligations incumbent on the Union and its Member States.

Justification

Given the cross border nature of cyber incidents, ENISA should act together with cybersecurity actors in Europe such as NATO where it is appropriate to do so. This is especially important as NATO may have cyber capabilities that ENISA does not have and vice versa. In the context of increased cyber attacks being directed against states as a whole, it is imperative for Europe's security that ENISA cooperates with international organisations such as NATO at the international level.

Amendment 160

Proposal for a regulation Article 41 – paragraph 2

Text proposed by the Commission

2. The Agency's host Member State shall provide the best possible conditions to ensure the proper functioning of the Agency, including the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses.

Amendment

2. The Agency's host Member State shall provide the best possible conditions to ensure the proper functioning of the Agency, including ***a single location for the entire Agency***, the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses.

Justification

The current structure of the agency with its administrative seat in Heraklion and the core operations in Athens has proven ineffective and costly. All ENISA staff should therefore be working in the same city. Given the criteria mentioned in this paragraph, this location should be Athens.

Amendment 161

Proposal for a regulation Article 43 – paragraph 1

Text proposed by the Commission

A European cybersecurity certification scheme shall attest that the ICT products

Amendment

A European cybersecurity certification scheme shall attest that the ICT products,

and services *that have been certified in accordance with such scheme* comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and **systems**.

processes and services covered have no known vulnerabilities at the time of certification, and comply with specified requirements *that may refer to European and international standards, technical specification and ICT technical specification*’ as regards their ability to resist, **throughout their life cycle**, at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and **meet the specified security objectives**.

Amendment 162

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

Text proposed by the Commission

Amendment

-1. The Commission shall adopt delegated acts in accordance with Article 55a, supplementing this Regulation by establishing a Union rolling work programme for European cybersecurity certification schemes. Those delegated acts shall identify common actions to be undertaken at Union level and strategic priorities. The Union rolling work programme shall in particular include a priority list of ICT products, processes and services suitable for being subject to a European cybersecurity certification scheme as well as an analysis as to whether there is an equivalent level of quality, know-how and expertise among the conformity assessment bodies and the national certification supervisory authorities and, if necessary, a proposal of measures how such a level of equivalence is to be achieved.

The initial Union rolling work programme shall be established no later than ... [six months after entry into force

of this Regulation] and shall be updated as necessary but in any event at least every two years thereafter. The Union rolling work programme shall be made publicly available.

Prior to adopting or updating the Union rolling work programme, the Commission shall consult the Member States' Certification Group, the Agency and the Stakeholders' Certification Group by means of an open, transparent and inclusive consultation.

Amendment 163

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

Text proposed by the Commission

Amendment

-1a. When justified, the Commission may request the Agency to draft a candidate European cybersecurity certification scheme. The request shall be based on the Union rolling work programme.

Amendment 164

Proposal for a regulation Article 44 – paragraph 1

Text proposed by the Commission

Amendment

1. *Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.*

1. *The request for a candidate European cybersecurity certification scheme shall contain the scope, the applicable security objectives referred to in Article 45, the applicable elements referred to in Article 47, and a deadline by which the specific candidate scheme is to become effective. While drafting the request, the Commission may consult the Agency, the Member States Certification Group and the Stakeholders Certification Group.*

Amendment 165

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 **the** candidate schemes referred to in paragraph - **1 (new)**, **the Agency** shall consult all relevant stakeholders **by means of a formal, open, transparent and inclusive consultation processes and shall** closely cooperate with the **Member States Certification Group, the Stakeholder Certification Group, ad-hoc committees in accordance with Article 20a of this Regulation and the European Standardisation Bodies**. They shall provide **the Agency** with the assistance and expert advice required by **the Agency** in relation to the preparation of the candidate scheme, including by providing opinions where necessary.

Amendment 166

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. **The Agency** shall transmit the candidate scheme prepared in accordance with **paragraphs 1 and 2 of this Article** to the Commission.

Amendment 167

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

Amendment

4. The Commission, based on the candidate scheme proposed by **the Agency**, may adopt **delegated** acts, in accordance

accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.

with Article 55a, **supplementing this Regulation** by providing for European cybersecurity certification schemes for ICT products, **processes** and services meeting the requirements of Articles 45, 46 and 47.

Amendment 168

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. **The Agency** shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes, **including with regard to withdrawn and expired certificates, and national certifications covered.**

Where a European cybersecurity certification scheme satisfies the requirements with which it aims to comply in accordance with the relevant Union harmonisation law, the Commission shall, without delay, publish a reference thereof in the Official Journal of the European Union and by any other means in accordance with the conditions laid down in the corresponding act of Union harmonisation law.

Amendment 169

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

Text proposed by the Commission

Amendment

5 a. The Agency shall review in accordance with the structure established under this Regulation the adopted schemes at the end of their validity in accordance with Article 47(1.ac) or upon the request from the Commission, taking into account feedback received from

relevant stakeholders.

Amendment 170

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

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

Amendment 171

Proposal for a regulation

Article 45 – paragraph 1 – point a

Text proposed by the Commission

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

Amendment

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

Amendment 172

Proposal for a regulation

Article 45 – paragraph 1 – point b

Text proposed by the Commission

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

Amendment

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

Amendment 173

Proposal for a regulation

Article 45 – paragraph 1 – point c

Text proposed by the Commission

Amendment

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

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

Amendment 174

Proposal for a regulation

Article 45 – paragraph 1 – point d

Text proposed by the Commission

Amendment

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

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

Amendment 175

Proposal for a regulation

Article 45 – paragraph 1 – point e

Text proposed by the Commission

Amendment

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

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

Amendment 176

Proposal for a regulation

Article 45 – paragraph 1 – point f

Text proposed by the Commission

Amendment

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

(f) ***that ICT products, processes and services are secure by default and by design***

Amendment 177

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

Text proposed by the Commission

(g) **ensure** that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates.

Amendment

(g) that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates.

Amendment 178

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

Text proposed by the Commission

Amendment

(g a) that other risks linked to cyber-incidents, such as risks to life, health, the environment and other significant legal interests are minimised.

Amendment 179

Proposal for a regulation
Article 46 – paragraph 1

Text proposed by the Commission

Amendment

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

1. A European cybersecurity certification scheme may specify one or more of the following ***risk-based*** assurance levels ***according to the context and intended use of the ICT products, processes and services***: basic, substantial and/or high, for ICT products, ***processes*** and services issued under that scheme.

Amendment 180

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

Text proposed by the Commission

(a) assurance level basic shall *refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a limited degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents;*

Amendment 181

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 182

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*

Amendment

(a) ***The*** assurance level basic shall ***correspond to a low risk, in terms of the combined likelihood and damage, related to an ICT product, process and service having regard to their intended use and context. The assurance level basic provides the confidence that the known basic risks of cyber incidents can be resisted.***

Amendment

(b) ***The*** assurance level substantial shall ***correspond to a higher risk, in terms of the combined likelihood and damage, related to an ICT product, process and service. The assurance level substantial provides the confidence that known risks of cyber incidents can be prevented and that there is also capability to resist cyber-attacks with limited resources.***

Amendment

(c) ***The*** assurance level high shall ***correspond to a high risk in terms of the damage related to an ICT product, process and service. The assurance level high***

of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service than certificates with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity incidents.

provides the confidence that risks of cyber incidents can be prevented and that there is also capability to resist state-of-the-art cyber-attacks with significant resources.

Amendment 183

Proposal for a regulation Article 46 a (new)

Text proposed by the Commission

Amendment

Article 46 a

Evaluation of assurance levels of European cybersecurity certification schemes

- 1. For the assurance level basic, the manufacturer or provider of ICT products, processes and services may, under its sole responsibility, perform a self-assessment of conformity.*
- 2. For the assurance level substantial, the evaluation shall be guided at least by the verification of the conformity of security functionalities of the product, process or service to its technical documentation;*
- 3. For the assurance levels high, the evaluation methodology shall be guided at least by efficiency testing which assesses the resistance of security functionalities against attackers having significant resources*

Amendment 184

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

Text proposed by the Commission

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

Amendment

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

Amendment 185

Proposal for a regulation

Article 47 – paragraph 1 – point a a (new)

Text proposed by the Commission

Amendment

(a a) scope and cybersecurity requirements, and when applicable, that scope and those requirements shall mirror those of the national cybersecurity certifications that it replaces, or are provided for in legal acts;

Amendment 186

Proposal for a regulation

Article 47 – paragraph 1 – point a b (new)

Text proposed by the Commission

Amendment

(a b) the validity period of the certification scheme;

Amendment 187

Proposal for a regulation

Article 47 – paragraph 1 – point b

Text proposed by the Commission

Amendment

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

(b) detailed specification of the cybersecurity requirements against which the specific ICT products, ***processes*** and services are evaluated, for example by reference to ***European*** or international standards, technical specifications ***or ICT technical specifications, defined in such a***

way that certification can be built into or based on the producer's systematic security processes followed during the development and lifecycle of the product or service in question;

Amendment 188

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

Text proposed by the Commission

Amendment

(b a) information of known cyber threats that are not covered by the certification and guidance to deal with them;

Amendment 189

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

Text proposed by the Commission

Amendment

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

(c) where applicable, one or more assurance levels *taking into account inter alia a risk-based approach;*

Amendment 190

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

Text proposed by the Commission

Amendment

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

Amendment 191

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

Text proposed by the Commission

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

Amendment

(d) specific evaluation criteria, ***types of conformity assessment*** and methods, in order to demonstrate that the specific objectives referred to in Article 45 are achieved;

Amendment 192

Proposal for a regulation

Article 47 – paragraph 1 – point e

Text proposed by the Commission

(e) information to be supplied to the conformity assessment bodies by an applicant which is necessary for certification;

Amendment

(e) information to be supplied to the conformity assessment bodies by an applicant which is necessary for certification;

Amendment 193

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) ***cybersecurity information pursuant to Article 47a of this Regulation;***

Amendment 194

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;

Amendment 195

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, **reviewing**, extending and reducing the scope **and the validity period of the certificate**;

Amendment 196

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

Text proposed by the Commission

Amendment

(h a) rules aiming to treat vulnerabilities that may arise after the certification is issued by establishing a dynamic and continuous organisational process, involving providers and users;

Amendment 197

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 **self-assessed and** certified ICT products and services with the certification requirements;

Amendment 198

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

Text proposed by the Commission

(j) rules concerning how **previously undetected** cybersecurity vulnerabilities in

Amendment

(j) rules concerning how **not publicly known** cybersecurity vulnerabilities in ICT

ICT products and services are to be reported and dealt with;

products and services are to be reported and dealt with *once detected*;

Amendment 199

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 covering the same type or categories of ICT products, *processes* and services, *security requirements and evaluation criteria and methods*;

Amendment 200

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

Text proposed by the Commission

Amendment

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

Amendment 201

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

Text proposed by the Commission

Amendment

1 a. Maintenance processes with updates shall not render certification invalid, unless such updates have a substantial adverse effect on the security of the ICT product, process or service.

Amendment 202

Proposal for a regulation Article 47 a (new)

Article 47 a

Cybersecurity information for certified products, process and services

- 1. The manufacturer or provider of ICT products, processes and services falling under a certification scheme pursuant to this Regulation shall provide the end user with a document, in electronic or paper form, containing at least the following information: the assurance level of the certificate relating to the intended use of the ICT product, process or service; a description of the risks that the certification is intended to provide confidence in resisting against; recommendations on how users can further foster the cybersecurity of the product, process or service, the regularity of and the support period following any updates; where applicable, information about how users can preserve the main features of the product, process or service in case of an attack.***
- 2. The document referred to in paragraph 1 of this Article shall be available throughout the lifecycle of the product, process or services until its discontinuity from the market and for a minimum period of five years.***
- 3. The Commission shall adopt implementing acts establishing a template for the document. The Commission may request the Agency to propose a candidate template. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 55 of this Regulation.***

Amendment 203

**Proposal for a regulation
Article 48 – paragraph 1**

Text proposed by the Commission

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

Amendment

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

Amendment 204

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, **and only** 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 **a body that is accredited as a conformity assessment body pursuant to Article 51, paragraph 1 of this Regulation. The natural or legal person which submits its ICT products or services to the certification mechanism shall make available to the conformity assessment body referred to in Article 51 all information necessary to conduct the certification procedure.**

Amendment 205

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

Amendment

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

conduct the certification procedure.

information necessary to conduct the certification procedure, **including information on any known security vulnerabilities. The submission can be made with any conformity assessment body referred to in Article 51.**

Amendment 206

Proposal for a regulation Article 48 – paragraph 6

Text proposed by the Commission

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

Amendment

6. Certificates shall be issued for a maximum period **determined on a case by case basis by each scheme, taking into account a reasonable life-cycle which shall not exceed in any case five years** and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.

Justification

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

Amendment 207

Proposal for a regulation Article 48 – paragraph 7

Text proposed by the Commission

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

Amendment

7. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States **as satisfying local cybersecurity requirements relating to ICT products and processes and consumer electronic devices covered by that certificate, taking into account the specified assurance level referred to in Article 46, and there shall be no discrimination between such certificates based either on the Member State of origin or the issuing conformity assessment body referred to in Article 51.**

Justification

In order to avoid fragmentation in the recognition and/ or conformity of EU cybersecurity certification schemes, the Article needs to emphasise that no the place of issuance of a certificate shall not be subject to discrimination.

Amendment 208

Proposal for a regulation Article 48 a (new)

Text proposed by the Commission

Amendment

Article 48 a

Certification schemes for operators of essential services

1. When European cybersecurity certifications schemes have been adopted pursuant to paragraph 2 of this Article, operators of essential services shall, in order to comply with the security requirements pursuant to Article 14 of the Directive (EU) 2016/1148, use products, processes and services covered by those certification schemes.

2. By [one year after the entry into force of this Regulation] the Commission shall, after consulting the Cooperation Group referred to in Article 11 of the Directive (EU) 2016/1148, adopt delegated acts in accordance with Article 55a, supplementing this Regulation by listing the categories of products, processes and services, that meet both of the following criteria:

(a) they are intended for use by operators of essential services; and

(b) their malfunctioning would have a significant disruptive effect on the provision of the essential service.

3. The Commission shall adopt delegated acts in accordance with Article 55a, amending this Regulation by updating, when necessary, the list of categories of products, processes and services referred to in paragraph 3 of this

Article.

4. The Commission shall request the Agency to draft a candidate European cybersecurity schemes pursuant to Article 44(-1) of this Regulation for the list of categories of products, processes and services referred in paragraphs 2 and 3 of this Article as soon as that list is adopted or updated. The certificates issued pursuant to such European cybersecurity certification schemes shall have an assurance level high.

Amendment 209

Proposal for a regulation Article 48 b (new)

Text proposed by the Commission

Amendment

Article 48 b

Formal objections to European cybersecurity certification schemes

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

(a) to publish, not to publish or to publish with restriction the references to the European cybersecurity scheme concerned in the Official Journal of the European Union;

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

of the European Union.

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

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

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

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

Amendment 210

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, **processes** 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, **processes** and services not covered by a European cybersecurity certification scheme shall continue to exist.

Amendment 211

Proposal for a regulation Article 49 – paragraph 2

Text proposed by the Commission

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products and services covered by a European cybersecurity certification scheme in force.

Amendment

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, **processes** and services covered by a European cybersecurity certification scheme in force.

Amendment 212

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

Text proposed by the Commission

Amendment

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

Amendment 213

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

Text proposed by the Commission

Amendment

3 b. Member States shall, upon request, send draft national cybersecurity certification schemes to other Member States, the Agency or the Commission, at least in electronic form.

Amendment 214

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

Text proposed by the Commission

Amendment

3 c. Without prejudice of Directive (EU) 2015/1535, Member States shall, within three months, reply to, and take due account of, any observation received from any other Member State, the Agency or the Commission with respect to any draft referred to in paragraph 3b of this Article.

Amendment 215

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

Text proposed by the Commission

Amendment

3 d. When observations received pursuant to paragraph 3c of this Article indicate that a draft national cybersecurity certification scheme is likely to have a negative impact on the proper functioning of the internal market, the receiving Member State shall consult and take utmost account of the observations of the Agency and the Commission before adopting the draft scheme.

Amendment 216

Proposal for a regulation Article 50 – paragraph 5

Text proposed by the Commission

Amendment

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

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

Amendment 217

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 *verify* 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 218

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 relation to the notification of conformity assessment bodies and the related tasks set out in Article 52 of this Regulation;

Amendment

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

Amendment 219

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

Text proposed by the Commission

Amendment

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

Justification

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

Amendment 220

Proposal for a regulation

Article 50 – paragraph 6 – point c

Text proposed by the Commission

Amendment

(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;

(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-assessment 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 221

Proposal for a regulation

Article 50 – paragraph 6 – point c a (new)

Text proposed by the Commission

Amendment

(ca) report the results of verifications under point (a) and the assessments under point (b) to the Agency and the European Cybersecurity Certification Group;

Amendment 222

Proposal for a regulation

Article 50 – paragraph 6 – point d

Text proposed by the Commission

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

Amendment

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

Amendment 223

Proposal for a regulation

Article 50 – paragraph 6 – point d

Text proposed by the Commission

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

Amendment

(d) cooperate with other national certification supervisory authorities or other public ***authorities, such as national data protection supervisory*** authorities, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific European ***IT security*** certification schemes;

Justification

From the EDPS opinion.

Amendment 224

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 225

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 226

Proposal for a regulation Article 50 – paragraph 8

Text proposed by the Commission

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

Amendment

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

Amendment 227

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

Text proposed by the Commission

Amendment

8a. Each national certification supervisory authority, and each member and staff of each national certification supervisory authority, shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the

performance of their tasks or the exercise of their powers.

Amendment 228

Proposal for a regulation Article 50 a (new)

Text proposed by the Commission

Amendment

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 organised by the Agency.*
- 2. Peer evaluation shall be operated on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints. Appropriate appeal procedures against decisions taken as a result of such evaluation shall be provided for.*
- 3. Peer review shall cover the assessments of the procedures put in place by national certification supervisory authorities, in particular the procedures for checking compliance of the certificates, the procedures for monitoring and supervising the activities of conformity assessment bodies, 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 the national certification supervisory authorities in question have sufficient resources for the proper performance of their duties as required by Article 50(4).*
- 4. 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. the Agency may participate in the peer review and shall decide on its participation on the basis of a risk assessment analysis.

5. The Commission may adopt delegated acts in accordance with Article 55a, supplementing this Regulation by establishing 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 Member States' Certification Group.

6. The outcome of the peer review shall be examined by the Member States' Certification Group. The Agency shall draw up a summary of the outcome and when necessary provide guidance and best practice documents and make them public.

Amendment 229

Proposal for a regulation Article 51 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. For the assurance level high, the conformity assessment body must, in addition to its accreditation, be notified by the national certification supervisory authority with regard to its competence and expertise in the assessment of cybersecurity. The national certification supervisory authority shall carry out regular audits of the expertise and competences of the notified conformity assessment bodies.

Justification

High levels of assurance require effectiveness testing. The expertise and competences of the conformity assessment bodies carrying out effectiveness tests must be regularly audited to ensure in particular the quality of the tests.

Amendment 230

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

Text proposed by the Commission

Amendment

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

Amendment 231

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

Text proposed by the Commission

Amendment

2b. Where manufacturers opt for a ‘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 232

Proposal for a regulation Article 52 – paragraph 5

Text proposed by the Commission

Amendment

5. The Commission may, by means of ***implementing*** acts, define the circumstances, formats and procedures of notifications referred to in paragraph 1 of

5. The Commission may, by means of ***delegated*** acts, define the circumstances, formats and procedures of notifications referred to in paragraph 1 of this Article.

this Article. Those **implementing** acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Those **delegated** acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Amendment 233

Proposal for a regulation Article 53 – title

Text proposed by the Commission

European Cybersecurity Certification Group

Amendment

Member States Certification Group

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

Amendment 234

Proposal for a regulation Article 53 – paragraph 1

Text proposed by the Commission

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

Amendment

1. The **Member States Certification Group** shall be established.

Amendment 235

Proposal for a regulation Article 53 – paragraph 2

Text proposed by the Commission

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

Amendment

2. The **Member States Certification Group** shall be composed of national certification supervisory authorities (**NCSAs**) **from each Member States**. The authorities shall be represented by the heads or by other high level representatives of national certification supervisory authorities. **Members of the Stakeholders Certification Group may be invited to**

meetings of the Group and to participate in its work.

Amendment 236

Proposal for a regulation

Article 53 – paragraph 3 – introductory part

Text proposed by the Commission

3. The Group shall have the following tasks:

Amendment

3. The ***Member States Certification*** Group shall have the following tasks:

Amendment 237

Proposal for a regulation

Article 53 – paragraph 3 – point b

Text proposed by the Commission

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

Amendment

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

Amendment 238

Proposal for a regulation

Article 53 – paragraph 3 – point d a (new)

Text proposed by the Commission

Amendment

(d a) to adopt recommendations determining the intervals at which national certification supervisory authorities are to carry out verifications of certificates and self-assessment 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 239

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

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

Amendment 240

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

Text proposed by the Commission

Amendment

(f a) to facilitate the alignment of European cybersecurity schemes with internationally recognised standards, including by reviewing existing European cybersecurity schemes and, where appropriate, making recommendations to the Agency to engage with relevant international standardisation organisations to address insufficiencies or gaps in available internationally recognised standards;

Amendment 241

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

Text proposed by the Commission

Amendment

(f b) to establish a peer review process. This process shall have regard in particular to the required technical expertise of NCSAs in the fulfilment of their tasks, as referred in Articles 48 and 50, and include when necessary the development of guidance and best practice documents to improve the compliance of the NCSAs with this Regulation;

Amendment 242

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

Text proposed by the Commission

Amendment

(f c) to supervise the monitoring and maintenance of certificates;

Amendment 243

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

Text proposed by the Commission

Amendment

(f d) to take into account the results of stakeholder consultation conducted in the preparation of a candidate scheme, in accordance with Article 44.

Amendment 244

Proposal for a regulation Article 53 – paragraph 4

Text proposed by the Commission

Amendment

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

4. The Commission shall chair the ***Member States Certification*** Group and provide the secretariat to it, with the assistance of ***the Agency*** as provided for in Article 8(a).

Amendment 245

Proposal for a regulation Article 53 a (new)

Text proposed by the Commission

Amendment

Article 53a

Right to an effective judicial remedy against a supervisory authority or

conformity assessment body

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy:

(a) against a decision of a conformity assessment body or national certification supervisory authority concerning them, including, where applicable, in relation to the issuing, non-issuing or recognition of a European cybersecurity certificate which such person holds; and

(b) where a national certification supervisory authority does not deal with a complaint for which it is competent.

2. Proceedings against a conformity assessment body or national certification supervisory authority shall be brought before the courts of the Member State where the conformity assessment body or the national certification supervisory authority is established.

Amendment 246

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

Text proposed by the Commission

Amendment

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

Amendment 247

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

Text proposed by the Commission

Amendment

Article 55 a

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to

the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 44 and 48a shall be conferred on the Commission for an indeterminate period of time from ... [date of entry into force of the basic legislative act].

3. The delegation of power referred to in Articles 44 and 48a 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.

4. 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 on Better Law-Making of 13 April 2016.

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

6. A delegated act adopted pursuant to Articles 44 and 48a shall enter into force only if no objection has been expressed either by the European Parliament or by 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.

Proposal for a regulation
Article 56 – paragraph 1

Text proposed by the Commission

1. Not later than **five** years after the date referred to in Article 58, and every **five** years thereafter, the Commission shall assess the impact, effectiveness and efficiency of the Agency and its working practices and the possible need to modify the mandate of the Agency and the financial implications of any such modification. The evaluation shall take into account any feedback made to the Agency in response to its activities. Where the Commission considers that the continuation of the Agency is no longer justified with regard to its assigned objectives, mandate and tasks, it may propose that this Regulation be amended with regard to the provisions related to the Agency.

Amendment 249

Proposal for a regulation
Article 56 – paragraph 2

Text proposed by the Commission

2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products and services in the Union and improving the functioning of the internal market.

Amendment 250

Proposal for a regulation
Article 56 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

1. Not later than **two** years after the date referred to in Article 58, and every **two** years thereafter, the Commission shall assess the impact, effectiveness and efficiency of the Agency and its working practices and the possible need to modify the mandate of the Agency and the financial implications of any such modification. The evaluation shall take into account any feedback made to the Agency in response to its activities. Where the Commission considers that the continuation of the Agency is no longer justified with regard to its assigned objectives, mandate and tasks, it may propose that this Regulation be amended with regard to the provisions related to the Agency.

Amendment

2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, **processes** and services in the Union and improving the functioning of the internal market.

Amendment

2 a. The evaluation shall assess whether

cybersecurity essential requirements for access to the internal market are necessary in order to prevent products, services and processes entering the Union market which do not meet basic cybersecurity requirements.

Amendment 251

Proposal for a regulation Annex -I (new)

Text proposed by the Commission

Amendment

ANNEX -I

Upon launching the EU cybersecurity certification framework it is likely that attention focuses on areas of imminent interest to rise to the challenge posed by emerging technologies. The area of the Internet of Things is of particular interest as it cuts across consumer as well as industry requirements. The following priority list for adoption into the certification framework is proposed:

- (1) Certification of cloud service provision.*
- (2) Certification of IoT devices including:*
 - a. devices at individual level, such as smart wearables;*
 - b. devices at community level, such as smart cars, smart homes, health devices;*
 - c. devices at society level such as smart cities and smart grids.*
- (3) Industry 4.0 involving intelligent, interconnected cyber-physical systems that automate all phases of industrial operations, spanning from design and manufacturing to operation, supply chain and service maintenance.*
- (4) Certification of technologies and products exploited in every-day life. Such an example could be networking devices, such as home internet routers.*

Amendment 252

Proposal for a regulation Annex I – paragraph 1 – point 5 a (new)

Text proposed by the Commission

Amendment

5a. If a conformity assessment body is owned or operated by a public entity or institution, independence and absence of any conflict of interest shall be ensured and documented between, on the one hand, the certification supervisory authority and, on the other hand, the conformity assessment body.

Amendment 253

Proposal for a regulation Annex I – paragraph 1 – point 8

Text proposed by the Commission

Amendment

8. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.

8. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. ***Any subcontracting or consultation of external personnel shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.***

Amendment 254

Proposal for a regulation Annex I – paragraph 1 – point 12

Text proposed by the Commission

12. The impartiality of the conformity assessment bodies, of their top-level management and of the assessment personnel shall be guaranteed.

Amendment

12. The impartiality of the conformity assessment bodies, of their top-level management and of the assessment personnel **and subcontractors** shall be guaranteed.

Amendment 255

Proposal for a regulation Annex I – paragraph 1 – point 15

Text proposed by the Commission

15. The personnel of a conformity assessment body shall observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation or pursuant to any provision of national law giving effect to it, except in relation to the competent authorities of the Member States in which its activities are carried out.

Amendment

15. ***The conformity assessment body and its personnel, committees, subsidiaries, subcontractors, and any associated body or personnel of external bodies*** of a conformity assessment body shall ***maintain confidentiality and*** observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation or pursuant to any provision of national law giving effect to it, except ***where disclosure is required by Union or Member State law to which such persons are subject except*** in relation to the competent authorities of the Member States in which its activities are carried out. ***Proprietary rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this Section 15.***

Amendment 256

Proposal for a regulation Annex I – paragraph 1 – point 15 a (new)

Text proposed by the Commission

Amendment

15a. With the exception of Section 15, the requirements of this Annex in no way preclude exchanges of technical information and regulatory guidance

between a conformity assessment body and a person applying, or considering whether to apply, for certification.

Amendment 257

Proposal for a regulation
Annex I – paragraph 1 – point 15 b (new)

Text proposed by the Commission

Amendment

15b. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of small and medium-sized enterprises as defined in Recommendation 2003/361/EC in relation to fees.