European Parliament
2014-2019

Plenary sitting

A8-0264/2018

30.7.2018

***|
REPORT

on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Committee on Industry, Research and Energy

Rapporteur: Angelika Niebler

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

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

Symbols for procedures

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

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

Amendments to a draft act

Amendments by Parliament set out in two columns

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

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

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.
By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

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

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

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

– having regard to the opinion of the European Economic and Social Committee of 14 February 2018[1],

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

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

– having regard to the report of the Committee on Industry, Research and Energy and the opinions of the Committee on the Internal Market and Consumer Protection, the Committee on Budgets and the Committee on Civil Liberties, Justice and Home Affairs (A8-0264/2018),

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

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

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

[1] OJ C 227, 28.6.2018, p. 86.

Amendment 1

Proposal for a regulation
Recital 1

Text proposed by the Commission	*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 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.	(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	*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,	(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***, processes*** and

undermining trust in digital solutions.	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	*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.	(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. ***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	*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 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.	(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	*Amendment*
(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given	(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.

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.	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

Text proposed by the Commission	*Amendment*
(7) The Union has already taken important steps to ensure cybersecurity and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to cybersecurity threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of	(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.

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	*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 within the framework of the new Union cybersecurity policy, it is necessary to	(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***

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.

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	*Amendment*
(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.	(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	*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	(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.	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 Members 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	*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	(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.	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	*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, 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.	(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	*Amendment*
(15) The Agency should assist the Member States and Union institutions,	(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.

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	*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 ***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	(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

Network.	CSIRTs Network.

Amendment 20

Proposal for a regulation
Recital 19

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

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	*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. 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.	(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	*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,	(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.

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

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.

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)

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

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.

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

Director and decide on the extension of the Executive Director's term of office and on the termination thereof.	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	*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.	(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	*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 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.	(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.

Amendment 36

Proposal for a regulation
Recital 44

Text proposed by the Commission	*Amendment*
(44) The Agency should have a	(44) The Agency should have a ***ENISA***

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.	***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	*Amendment*
(46) In order to guarantee the full autonomy and independence of the Agency and to enable it to perform additional and new tasks, including unforeseen emergency tasks, the Agency should be granted a sufficient and autonomous budget whose revenue comes primarily from a contribution from the Union and contributions from third countries participating in the Agency's work. The majority of the Agency staff should be directly engaged in the operational implementation of the Agency's mandate. The host Member State, or any other Member State, should be allowed to make voluntary contributions to the revenue of the Agency. The Union's budgetary procedure should remain applicable as far as any subsidies chargeable to the general budget of the Union are concerned. Moreover, the Court of Auditors should audit the Agency's accounts to ensure transparency ***and*** accountability.	(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 39

Proposal for a regulation
Recital 47

Text proposed by the Commission	*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	(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.

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	*Amendment*
(48) Cybersecurity certification plays an ***important*** role in increasing trust and	(48) ***European*** cybersecurity certification plays an ***essential*** role in

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.	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	*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 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 technologies that individuals and enterprises have access to. Similarly, in the	(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 cybersecurity technologies that individuals and enterprises have access to. Similarly,

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.

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	*Amendment*
(50) Currently, the cybersecurity certification of ICT products and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In this context, a certificate issued by one national cybersecurity authority is not in principle recognised by other Member States. Companies thus may have to certify their products and services in several Member States where they operate, for example with a view to participating in national procurement procedures. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach with regard to horizontal cybersecurity issues, for instance in the field of the Internet of Things. Existing schemes present significant shortcomings and differences in terms of product coverage, ***levels of*** assurance, substantive criteria and actual utilisation.	(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	*Amendment*
(52) In view of the above, it is necessary to establish a European cybersecurity certification framework laying down the main horizontal requirements for European cybersecurity certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping national cybersecurity certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should be non-discriminatory and based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.	(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	*Amendment*
(53) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products and services. These schemes should be implemented and supervised by national certification supervisory authorities and certificates issued within these schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or other private organisations should fall outside the scope of the Regulation. However, the bodies operating such schemes may propose to the Commission to consider such schemes as a basis for approving them as a European scheme.	(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)

Text proposed by the Commission	*Amendment*
	(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

Text proposed by the Commission	*Amendment*
(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	*Amendment*
(55) The purpose of European cybersecurity certification schemes should be to ensure that ICT products ***and*** services certified under such a scheme comply with specified requirements. Such requirements concern the ability to resist, at a given level of ***assurance***, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products ***and*** services. ICT products ***and*** services and related cybersecurity needs are so diverse that it is very difficult to come up with general cybersecurity requirements valid across the board. It is, therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, complemented by a set of specific cybersecurity objectives that need to be taken into account when 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.	(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	*Amendment*
(56) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services***. The Commission, based on*** the candidate ***scheme*** proposed by ENISA, should then be empowered to adopt the European cybersecurity certification ***scheme*** by means of ***implementing*** acts. Taking account of the general purpose and security objectives identified in this Regulation, European cybersecurity certification schemes ***adopted by the Commission*** should specify a minimum set of elements concerning the subject-matter, the scope and functioning of the individual scheme. These should include among others the scope and object of the cybersecurity certification, including the categories of ICT products and services 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.	(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	*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 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.	(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	*Amendment*
(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.	(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	*Amendment*
(59) It is necessary to require all Member States to designate one cybersecurity certification supervisory authority to supervise compliance of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory with the requirements of this Regulation and of the relevant cybersecurity certification schemes. National certification supervisory authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories, investigate to the extent appropriate the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable time period. Moreover, they should cooperate with other national certification supervisory authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.	(59) It is necessary to require all Member States to designate one cybersecurity certification supervisory authority to supervise compliance of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory with the requirements of this Regulation and of the relevant cybersecurity certification schemes***, 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	*Amendment*
(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	(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

Commission in its work to ensure a consistent implementation and application of the European 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.	advise and assist the Commission in its work to ensure a consistent implementation and application of the European 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	*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 and services.	(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	*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	(63) In order to specify further the criteria for the accreditation of conformity assessment bodies, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the

Commission. The Commission should carry out appropriate consultations during its preparatory work, including at expert level. Those consultations should be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	Commission. The Commission should carry out appropriate consultations during its preparatory work, including at expert level ***and with relevant stakeholders, as 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	*Amendment*
(65) ***The examination procedure should be used for the adoption of implementing acts*** on European cybersecurity certification schemes for ICT products and services; on modalities of carrying enquiries by the Agency; as well as on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national certification supervisory authorities to the Commission.	(65) ***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	*Amendment*
(66) The Agency’s operations should be evaluated independently. The evaluation	(66) The Agency’s operations should be evaluated ***continuously and*** independently.

should have regard to the Agency achieving its objectives, its working practices and the relevance of its tasks***. The evaluation*** should ***also assess the impact, effectiveness and efficiency*** of the ***European cybersecurity certification framework***.	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 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	*Amendment*
(a) lays down the objectives, tasks and organisational aspects of ***ENISA,*** the "***EU Cybersecurity*** Agency", hereinafter 'the Agency'; and	(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	*Amendment*
(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products and services in the Union***.*** ***Such framework shall apply*** without prejudice to specific provisions regarding voluntary ***or*** mandatory certification in other Union acts.	(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	*Amendment*
(1) 'cybersecurity' ***comprises*** all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;	(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	*Amendment*
(2) 'network and information system' means a system ***within the meaning of*** point (1) of Article 4 of Directive (EU) 2016/1148;	(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	*Amendment*
(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;	(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	*Amendment*
(4) ‘operator of essential services’ means a ***public or private entity*** as defined in point (4) of Article 4 of Directive (EU) 2016/1148;	(4) ‘operator of essential services’ means an ***operator of essential services*** as defined in point (4) of Article 4 of Directive (EU) 2016/1148;

Amendment 80

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

Text proposed by the Commission	*Amendment*
(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	(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	*Amendment*
(6) ‘incident’ means ***any event*** as defined in point (7) of Article 4 of Directive (EU) 2016/1148;	(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	*Amendment*
(7) ‘incident handling’ means ***any procedure*** as defined in point (8) of Article 4 of Directive (EU) 2016/1148;	(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	*Amendment*
(8) 'cyber threat' means any potential circumstance ***or*** event that may adversely impact network and information systems, their users and affected persons.	(8) 'cyber threat' means any potential circumstance***,*** event ***or any intentional 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 assessment body attesting that a given ICT product or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;	(10) 'European cybersecurity certificate' means a document issued by a conformity 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 Regulation (EU) No 1025/2012**.**	(16) 'standard ***, technical specification and ICT technical specification***' means a 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 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.	1. The Agency shall be a centre of ***theoretical and practical*** expertise on cybersecurity by virtue of its 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	*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.	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	*Amendment*
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.	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	*Amendment*
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.	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	*Amendment*
5. The Agency shall increase cybersecurity capabilities at Union level in order to complement the action of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents.	5. The Agency shall ***contribute to increasing*** cybersecurity capabilities at Union level in order to complement 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	*Amendment*
6. The Agency shall promote the use of certification, including by contributing to the establishment and maintenance of a	6. The Agency shall promote the use of certification ***with a view to avoiding fragmentation in the internal market and***

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**.**	***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	*Amendment*
7. The Agency shall promote a high level of awareness ***of*** citizens and businesses on issues related to the cybersecurity.	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	*Amendment*
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;	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	*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;	2. assisting Member States to implement consistently the Union policy and law regarding cybersecurity notably in relation to Directive (EU) 2016/1148, ***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 advice, as well as facilitating the exchange of best practices between competent authorities;	(2) the promotion of an enhanced level of security of electronic communications***,*** ***data storage and data processing***, including by providing expertise and advice, as well as facilitating the exchange of best practices between competent authorities;

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 guidance on available tools, procedure, as well as on how to address regulatory issues related to information sharing.	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, ***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	*Amendment*
1. The Agency shall support operational cooperation among ***competent public*** bodies, and between stakeholders.	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	*Amendment*
(b) providing, at their request, technical assistance in case of incidents having a	(b) providing, at their request, technical assistance in ***the form of information sharing and expertise in the*** case of

significant or substantial impact;	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	*Amendment*
Upon a request by ***two*** or more Member States concerned, and with the sole purpose of providing advice for the prevention of future incidents, the Agency shall provide support to or carry out an ex-post technical enquiry following notifications by affected undertakings of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148. The Agency shall also carry out such an enquiry upon a duly justified request from the Commission in agreement with the concerned Member States in case of such incidents affecting more than ***two*** Member States.	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	*Amendment*
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.	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	*Amendment*
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	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

basis) or NIS Directive Single Points of Contact (in accordance with NIS Directive Article 14 (5)); European Cybercrime Centre (EC3) at Europol, CERT-EU.	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	(c) supporting the technical handling of an incident or crisis, ***based on its own independent expertise and resources,***

Member States;	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	(2) assisting the Commission in providing the secretariat to the ***Member States*** Certification Group pursuant to

to Article 53 of this Regulation;	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 national certification supervisory authorities and the industry;	(3) compiling and publishing guidelines and developing good practices***, including on cyber hygiene principles*** concerning the cybersecurity requirements of ICT 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	*Amendment*
(b) facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products and services, as well as draw up, in collaboration with Member States, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148;	(b) 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	*Amendment*
(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;	(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	*Amendment*
(e) raise awareness of the public about cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens and organisations;	(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	*Amendment*
(g) organise, in cooperation with the Member States and Union institutions, bodies, offices and agencies regular ***outreach*** campaigns to ***increase cybersecurity and its visibility in the Union.***	(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	*Amendment*
(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;	(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	*Amendment*
(d) a ***Permanent Stakeholders'*** Group which shall exercise the functions set out in Article 20.	(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	*Amendment*
(e) assess and adopt the consolidated annual report on the Agency's activities and send both the report and its assessment by 1 July of the following year, to the European Parliament, the Council, the Commission and the Court of Auditors. The annual report shall include the accounts ***and*** describe how the Agency has met its performance indicators. The annual report shall be made public;	(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	*Amendment*
(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;	(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	*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 and having regard to sound budgetary management;	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	*Amendment*
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.	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	*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.	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	*Amendment*
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.	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	*Amendment*
1. The Management Board, acting on a proposal by the Executive Director, shall set up a ***Permanent Stakeholders'*** Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in the cybersecurity, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities.	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	*Amendment*
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.	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	*Amendment*
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.	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	*Amendment*
4. The term of office of the ***Permanent Stakeholders'*** Group's members shall be two-and-a-half years. Members of the Management Board may not be members of the ***Permanent Stakeholders'*** Group. Experts from the Commission and the Member States shall be entitled to be present at the meetings of the ***Permanent Stakeholders'*** Group and to participate in its work. Representatives of other bodies deemed relevant by the	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

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.	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	*Amendment*
5. The ***Permanent Stakeholders'*** Group shall advise the Agency in respect of the performance of its activities. It shall in particular advise the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on ***all*** issues related to the work programme.	5. The ***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, 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.	2. Members of the Management Board, 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	*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.	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	*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.	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	*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. These arrangements shall not create legal obligations incumbent on the Union and its Member States.	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	*Amendment*
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	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***

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.	***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	*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***.	A European cybersecurity certification scheme shall attest that the ICT products***,*** ***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	*Amendment*
2. When preparing candidate schemes referred to in paragraph ***1 of this Article, ENISA*** shall consult all relevant stakeholders ***and*** closely cooperate with the ***Group. The*** Group shall provide ***ENISA*** with the assistance and expert advice required by ***ENISA*** in relation to the preparation of the candidate scheme, including by providing opinions where	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***

necessary.	***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	*Amendment*
3. ***ENISA*** shall transmit the candidate ***European cybersecurity certification*** scheme prepared in accordance with ***paragraph 2 of this Article*** to the Commission.	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	*Amendment*
4. The Commission, based on the candidate scheme proposed by ***ENISA***, may adopt ***implementing*** acts, in accordance with Article ***55(1)***, providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 ***of this Regulation***.	4. The Commission, based on the candidate scheme proposed by ***the Agency***, may adopt ***delegated*** acts, in accordance 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	*Amendment*
5. ***ENISA*** shall maintain a dedicated website providing information on, and	5. ***The Agency*** shall maintain a dedicated website providing information

publicity of, European cybersecurity certification schemes.	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	*Amendment*
A European cybersecurity certification scheme shall be so designed to take into account, as applicable, ***the following*** security objectives:	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	*Amendment*
(a) ***protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure***;	(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	*Amendment*
(b) ***protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss or alteration***;	(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***	(d) ***that ICT products, processes and*** services ***do not contain known***

times and by whom;

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	*Amendment*
(g) ***ensure*** that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates.	(g) 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	*Amendment*
(a) assurance level basic shall ***refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a limited degree of confidence in the claimed or asserted cybersecurity qualities of*** an ICT product ***or*** service***, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of cybersecurity*** incidents***;***	(a) ***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 181

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

Text proposed by the Commission	*Amendment*
(b) assurance level substantial shall ***refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of*** an ICT product ***or*** service***, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of cybersecurity*** incidents***;***	(b) ***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 182

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

Text proposed by the Commission	*Amendment*
(c) assurance level high shall ***refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of*** an ICT product ***or*** service ***than certificates with*** the assurance level ***substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity*** incidents.	(c) ***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 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	*Amendment*
(a) subject-matter and scope of the certification, including the type or categories of ICT products and services covered;	(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	*Amendment*
(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;	(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	*Amendment*
(e) information to be supplied to the conformity assessment bodies by an applicant which is necessary for certification;	(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	*Amendment*
(f) ***where the scheme provides for marks or labels, the conditions under which such marks or labels may be used***;	(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	*Amendment*
(g) ***where surveillance is part of the scheme,*** the rules for monitoring compliance with the requirements of the certificates, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;	(g) The rules for monitoring compliance with the requirements of the certificates, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;

Amendment 195

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

Text proposed by the Commission	*Amendment*
(h) conditions for granting,	(h) conditions for granting,

maintaining, continuing, extending and reducing the scope ***of certification***;	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	*Amendment*
(i) rules concerning the consequences of non-conformity of certified ICT products and services with the certification requirements;	(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	*Amendment*
(j) rules concerning how ***previously undetected*** cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with;	(j) rules concerning how ***not publicly known*** cybersecurity vulnerabilities in ICT 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	*Amendment*
(l) identification of national cybersecurity certification schemes covering the same type or categories of ICT products and services;	(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)

Text proposed by the Commission	*Amendment*
	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	*Amendment*
1. ICT products and services that have been certified under a European cybersecurity certification scheme adopted	1. ICT products***, processes*** and services that have been certified under a European cybersecurity certification

pursuant to Article 44 shall be presumed to be compliant with the requirements of such scheme.	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	*Amendment*
4. By ***the*** way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such public body shall be ***one of the following:***	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	*Amendment*
5. The natural or legal person which submits its ICT products ***or*** services to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure.	5. The natural or legal person which submits its ICT products***,*** services ***or processes*** to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure***, including information on any known security vulnerabilities***. ***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	*Amendment*
6. Certificates shall be issued for a maximum period ***of three years*** and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.	6. Certificates shall be issued for 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	*Amendment*
7. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.	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 pursuing 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	*Amendment*
1. Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the 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.	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	*Amendment*
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.	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	*Amendment*
(a) monitor and enforce the application of the provisions under this Title at national level and ***supervise*** compliance ***of*** the certificates that have been issued by conformity assessment bodies established in their respective territories with the requirements set out in this Title and in the corresponding European cybersecurity certification scheme;	(a) monitor and enforce the application of the provisions under this Title at national level and ***verify*** compliance***, 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	*Amendment*
(b) monitor and supervise the activities of conformity assessment bodies for the purpose of this Regulation, including in relation to the notification of conformity assessment bodies and the related tasks set out in Article 52 of this Regulation;	(b) monitor 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	*Amendment*

(d) cooperate with other national certification supervisory authorities or other public authorities, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;	(d) cooperate with other national certification supervisory authorities 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	*Amendment*
(d) cooperate with other national certification supervisory authorities or other public authorities, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific European ***cybersecurity*** certification schemes;	(d) cooperate with other national certification supervisory authorities 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	*Amendment*
(e) to withdraw, in accordance with national law, certificates that are not compliant with this Regulation or a European cybersecurity certification scheme;	(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	*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 and services.	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	5. The Commission may, by means of

implementing acts, define the circumstances, formats and procedures of notifications referred to in paragraph 1 of this Article. Those ***implementing*** acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

delegated acts, define the circumstances, formats and procedures of notifications referred to in paragraph 1 of this Article. 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	*Amendment*
European Cybersecurity Certification Group	***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	*Amendment*
1. The ***European Cybersecurity*** Certification Group ***(the 'Group')*** shall be established.	1. The ***Member States*** Certification Group shall be established.

Amendment 235

Proposal for a regulation
Article 53 – paragraph 2

Text proposed by the Commission	*Amendment*
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	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

certification supervisory authorities.	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	*Amendment*
3. The Group shall have the following tasks:	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	*Amendment*
(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;	(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 Article50(6)

Amendment 239

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

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

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.

Amendment 248

Proposal for a regulation
Article 56 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	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 249

Proposal for a regulation
Article 56 – paragraph 2

Text proposed by the Commission	*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 and services in the Union and improving the functioning of the internal market.	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 250

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

Text proposed by the Commission	*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	*Amendment*
12. The impartiality of the conformity assessment bodies, of their top-level management and of the assessment personnel shall be guaranteed.	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	*Amendment*
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.	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 Stat 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.

EXPLANATORY STATEMENT

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

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

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

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

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

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

As regards ENISA, the Rapporteur believes that it is crucial to set the right framework if we want a strong and well-functioning Agency. The Rapporteur welcomes a strengthened role for ENISA, comprising its then permanent mandate and an increase of its budget and staff but also a realistic approach is needed, considering the still small number of experts employed by ENISA compared to the size of staff in some national certification supervisory authorities. ENISA`s task should continue to be that of arranging for operational cooperation, by considering expertise gained under the NIS-Directive, to continue supporting capacity building in Member states and to be a source of information. Further, ENISA needs to play a strong role in establishing European cyber security schemes together with the Member States and relevant stakeholders.

As regards the certification, the Rapporteur is in favour of a clearer scope of application of the proposal. Firstly, not only products and services should be covered by this Regulation, but the whole life-cycle. Thus, processes have also to be included in the scope of application. On the other hand, areas of competences from the Member States should be clearly excluded, namely where public security, defence, national security and the area of criminal law are concerned.

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

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

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

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

22.5.2018

OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM(2017)0477 – C8-0310-2017 – 2017/0225(COD))

Rapporteur: (*) Nicola Danti

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

SHORT JUSTIFICATION

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

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

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

In general, the Rapporteur welcomes the approach proposed by the European

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

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

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

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

  1) to strengthen the surveillance powers of ENISA: together with the Certification Group, ENISA should carry out assessments of the procedures put in place by the authorities responsible for the issuance of EU certificates;
  2) that the national certification supervisory authorities should carry out periodic assessments (at least every two years) on the EU certificates issued by conformity assessment bodies;
  3) to introduce common binding criteria to be defined by the Group for setting out the scale, scope and frequency with which national certification supervisory authorities should carry out assessments referred to under point 2.
- The Rapporteur believes that a mandatory **EU Trust Label** should be introduced for certified ICT products and services, which are intended for end users. This label could help raise awareness of cybersecurity and give companies with good cybersecurity credentials a competitive edge.

- The Rapporteur agrees with the uniform and harmonised approach taken by the Commission, but he is convinced that it should be more flexible and adaptable to the specific characteristics and vulnerabilities of each product or service - no "one size-

fits-all" principle. Therefore, the Rapporteur believes that **assurance levels** should be re-named and should be used also taking account of the intended use of ICT products and services. Similarly, the duration of **validity of the certificate** should be defined on a scheme-by-scheme basis.

- Each certification scheme should be designed in such a way as to stimulate and encourage all actors involved in the sector concerned to develop and adopt security standards, technical norms and **security-by-design and privacy-by-design principles**, at all stages of the product or service lifecycle.

AMENDMENTS

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

Amendment 1

Proposal for a regulation
Recital 1

Text proposed by the Commission	*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 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.	(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	*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	(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.	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 ***the*** trust in digital solutions ***that is essential for the establishment of the digital single market***.

Amendment 3

Proposal for a regulation
Recital 3

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

Amendment 4

Proposal for a regulation
Recital 4

Text proposed by the Commission	*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 defences.	(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***

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.

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

Amendment 5

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, ***the*** trust in the digital single	(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, ***given that cyber incidents***

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.

undermine trust ***in digital service providers and*** in the digital single market ***itself, especially among consumers, trust*** should be further improved by offering transparent information on the level of security of ICT products and services. This can be facilitated by ***standardised*** EU-wide certification***, relying on European or international standards and*** providing common cybersecurity requirements and evaluation criteria across national markets and sectors. ***Alongside Union-wide certification, there are a range of voluntary measures that the private sector itself should take to bolster trust in the security of ICT products and services, in particular in view of the growing availability of IoT devices. For example, more effective use should be made of encryption and other technologies as well as technologies to prevent successful cyber-attacks such as blockchain, in order to improve the security of end-users' data and communications and the overall security of network and information systems in the Union.***

Amendment 6

Proposal for a regulation
Recital 5 a (new)

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

from a reactive to a proactive approach to responding to threats by emphasising the prevention of successful cyber-attacks.

Amendment 7

Proposal for a regulation
Recital 7

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

cybersecurity.

Amendment 8

Proposal for a regulation
Recital 11

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

Amendment 9

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) The Agency should contribute towards raising the awareness of the public about risks related to cybersecurity and provide guidance on good practices for individual users aimed at citizens and organisations. The Agency should also contribute to promote best practices and solutions ***at the level of*** individuals and organisations by collecting and analysing publicly available information regarding significant incidents, and by compiling reports with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in	(28) The Agency should contribute towards raising the awareness of the public about risks related to cybersecurity and provide guidance on good practices for individual users aimed at citizens and organisations. The Agency should also contribute to promote ***cyber-hygiene*** best practices and solutions***, meaning simple routine measures that*** individuals and organisations ***can take to minimise the risks from cyber threats, such as multi-factor authentication, patching, encryption, and access management. The Agency should do this*** by collecting and analysing publicly available information regarding significant incidents, and by compiling ***and publishing*** reports ***and guidelines*** with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. The Agency should furthermore organise, in cooperation with

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.

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

Amendment 10

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) The Agency should encourage Member States and service providers to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal cybersecurity**.** In particular, service providers and product manufacturers should withdraw or recycle	(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***.

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

Amendment 11

Proposal for a regulation
Recital 36 a (new)

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

The Agency should regularly consult and work in cooperation with the European standardisation organisations, in particular when preparing European cybersecurity certification schemes.

Amendment 12

Proposal for a regulation
Recital 44

Text proposed by the Commission	*Amendment*
(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, 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.	(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations***, academia*** and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the attention of the Agency. ***In order to ensure proper involvement of stakeholders in the cybersecurity certification framework, the Permanent Stakeholders' Group should also give advice on which ICT products and services to cover in future European cybersecurity certification schemes, and should make proposals to the Commission to request the Agency to prepare candidate schemes on such ICT products and services, either on its own initiative or following submission of proposals from relevant stakeholders.*** The composition of the Permanent Stakeholders***'*** Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure ***efficient and equitable*** representation of stakeholders in the work of the Agency.

Amendment 13

Proposal for a regulation
Recital 46

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

Amendment 14

Proposal for a regulation
Recital 47

Text proposed by the Commission	*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***.	(47) Conformity assessment is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. For the purposes of this Regulation, certification should be considered as a type of conformity assessment regarding the cybersecurity features ***and practices comprised in*** a product, process, service, system, or a combination of those ("ICT products and services") by an independent third party ***or through a procedure of self-declaration of***

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.	***conformity***. Certification cannot guarantee per se that certified ICT products and services are cyber secure ***and the end user should be made aware of it***. It is rather a procedure and technical methodology to attest that ICT products and services ***as well as the underlying processes and systems*** have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example as specified in technical standards.

Amendment 15

Proposal for a regulation
Recital 48

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

Amendment 16

Proposal for a regulation
Recital 50

Text proposed by the Commission	*Amendment*
(50) Currently, the cybersecurity certification of ICT products and services	(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.	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***, 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.

Amendment 17

Proposal for a regulation
Recital 52

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

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

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. ***Where a European cybersecurity certification has replaced a national scheme, certificates issued under the European scheme should be accepted as valid in cases where certification under a national scheme was required.*** The schemes should ***be guided by security-by-design and the principles referred to in Regulation (EU) 2016/679. They should also*** be non-discriminatory and based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.

Amendment 18

Proposal for a regulation
Recital 52 a (new)

Text proposed by the Commission	*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 19

Proposal for a regulation
Recital 55

Text proposed by the Commission	*Amendment*
(55) The purpose of European cybersecurity certification schemes should be to ensure that ICT products and services	(55) The purpose of European cybersecurity certification schemes should be ***to contribute to a high level of end-user***

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.

protection and European competitiveness and to boost the level of security within the digital single market, and more specifically to ensure that ICT products and services certified under a scheme comply with specified requirements. Such requirements concern the ability to resist, at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those ***processes,*** products, services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products and services. ICT products and services and related cybersecurity needs are so diverse that it is very difficult to come up with general cybersecurity requirements valid across the board. It is, therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, complemented by a set of specific cybersecurity objectives that need to be taken into account when designing European cybersecurity certification schemes. The modalities with which such objectives will be achieved in specific ICT products and services should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications. ***It is of paramount importance that each European cybersecurity certification scheme be designed in such a way as to stimulate and encourage all actors involved in the sector concerned to develop and adopt security standards, technical norms and security-by-design principles, at all stages of the product or service lifecycle. Where the certification scheme provides for marks or labels, the conditions under which such marks or labels may be used have to be outlined. Such label, which could be in the form of***

a digital logo or QR code, would indicate the risks associated with the operation and use of ICT products and services and should be clear and easily understandable for the end-user.

Amendment 20

Proposal for a regulation
Recital 55 a (new)

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

Amendment 21

Proposal for a regulation
Recital 56

Text proposed by the Commission	*Amendment*
(56) ***The Commission*** should ***be empowered to request ENISA to prepare*** candidate schemes ***for specific ICT products or services.*** The Commission***, based on the candidate scheme proposed by ENISA, should then be empowered to adopt the European cybersecurity certification scheme by means of implementing acts***. Taking account of the general purpose and security objectives identified in this Regulation, European cybersecurity certification schemes	(56) ***ENISA*** should ***maintain a dedicated website with an easy-to-use online tool listing information on adopted schemes,*** candidate schemes***, and schemes requested by*** the Commission. Taking account of the general purpose and security objectives identified in this Regulation, European 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.

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***.	These should include among others the scope and object of the cybersecurity certification, including the categories of ICT products and services covered, the detailed specification of the cybersecurity requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods ***associated with the operation and use of an ICT product, process or service, their inherent risk*** as well as the intended level of assurance: ***functionally secure, that is, assurance levels having a functional degree of security, substantially secure, highly secure, or any combination thereof. The assurance levels should not suggest absolute security, so as not to mislead the end-user. Consideration should also be given to the full lifecycle of the product. In order to clarify which risks a particular product or service is designed to be able to withstand, ENISA should coordinate the compilation of a checklist listing the risks that the ICT process, product or service is expected to face by a given category of users in a particular environment.***

Amendment 22

Proposal for a regulation
Recital 56 a (new)

Text proposed by the Commission	*Amendment*
	(56 a) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services. The power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of establishing European cybersecurity certification schemes for ICT products and services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work,

including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. When adopting those delegated acts, the Commission should base the cybersecurity certification schemes for ICT products and services on any relevant candidate schemes proposed by ENISA. In order to underpin trust and predictability in, and raise public awareness of, the cybersecurity certification framework.

Amendment 23

Proposal for a regulation
Recital 56 b (new)

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

Amendment 24

Proposal for a regulation
Recital 58

Text proposed by the Commission	*Amendment*
(58) Once a European cybersecurity	(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.

certification scheme is adopted, manufacturers of ICT products or providers of ICT services should be able to submit an application for certification of their ***processes,*** products***,*** or services to a conformity assessment body of their choice***, or to declare themselves that their products or services are in conformity with the relevant European cybersecurity certification scheme***. Conformity assessment bodies should be accredited by an accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements. Accreditation bodies should revoke an accreditation of a conformity assessment body where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation. ***With a view to ensuring that accreditation is carried out uniformly across the European Union, national certification supervisory authorities should be subject to a peer review on the procedures for checking the compliance of the products that are subject to cybersecurity certification.***

Amendment 25

Proposal for a regulation
Recital 59

Text proposed by the Commission	*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	(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.

cybersecurity certification schemes. National certification supervisory authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories, investigate to the extent appropriate the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable time period. Moreover, they should cooperate with other national certification supervisory authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes. ***Furthermore, they should supervise and verify the compliance of the self-declarations of conformity and that European cybersecurity certificates have been issued by conformity assessment bodies with the requirements set out in this Regulation including the rules adopted by the European Cybersecurity Certification Group and the requirements set out in the corresponding European cybersecurity certification scheme. Effective cooperation among the national certification supervisory authorities is essential for the proper implementation of European cybersecurity certification schemes and of technical issues concerning the cybersecurity of ICT products and services. The Commission should facilitate that exchange of information by making available a general electronic information support system, for example the Information and Communication System on Market Surveillance (ICSMS) and the rapid alert system for dangerous non-food products (RAPEX) already used by market surveillance authorities pursuant to Regulation (EC) No 765/2008.***

Amendment 26

Proposal for a regulation
Recital 63

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

Amendment 27

Proposal for a regulation
Recital 65

Text proposed by the Commission	*Amendment*
(65) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT products 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	(65) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT ***processes,*** products and services; on modalities of carrying enquiries by the Agency; as well as on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national certification supervisory

Commission.	authorities to the Commission***, taking into account the proven effectiveness of the electronic notification tool "New Approach Notified and Designated Organisations" (NANDO)***.

Amendment 28

Proposal for a regulation
Recital 66

Text proposed by the Commission	*Amendment*
(66) The Agency's operations should be evaluated independently. The evaluation should ***have regard to the Agency achieving its objectives,*** its working practices and the relevance of its tasks. The evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework.	(66) The Agency's operations should be evaluated independently. The evaluation should ***include the legitimacy and effectiveness of the agency's expenditure, its efficiency in reaching its targets and a description of*** its working practices and the relevance of its tasks. The evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework.

Amendment 29

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

Text proposed by the Commission	*Amendment*
(11) 'ICT product and service' means ***any*** element ***or group of elements*** of network and information systems;	(11) 'ICT ***process,*** product and service' means ***a product, service, process, system, or a combination thereof that is an*** element of network and information systems; *(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)*

Amendment 30

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

Text proposed by the Commission	*Amendment*
	(11 a) "national certification supervisory authority" means an authority of a Member State responsible for carrying out monitoring, enforcement and supervisory tasks in relation to cybersecurity certification on its territory;

Amendment 31

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

Text proposed by the Commission	*Amendment*
	(16 a) 'self-declaration of conformity' means a statement by the manufacturer that their ICT process, product or service conforms with a specified European cybersecurity certification schemes.

Amendment 32

Proposal for a regulation
Article 3 – paragraph 1

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

Amendment 33

Proposal for a regulation
Article 4 – paragraph 5

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

Amendment 34

Proposal for a regulation
Article 4 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Agency shall promote the use of certification***, including by contributing*** to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III ***of this Regulation***, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus ***strengthen*** trust in the digital ***internal*** market.	6. The Agency shall promote the use of certification ***while avoiding the fragmentation caused by lack of coordination between existing certification schemes in the Union. The Agency shall contribute*** to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with ***Articles 43 to 54 [***Title III***]***, with a view to increasing ***the*** transparency of cybersecurity assurance of ICT products and services and thus ***strengthening*** trust in the digital ***single*** market.

Amendment 35

Proposal for a regulation
Article 4 – paragraph 7

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

Amendment 36

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

Text proposed by the Commission	*Amendment*
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;	1. assisting and advising on the development and review of Union policy and law in the area of cybersecurity, as well as sector-specific policy and law initiatives where matters related to cybersecurity are involved;

Justification

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

Amendment 37

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

Text proposed by the Commission	*Amendment*
	2a. assisting the European Data Protection Board established by Regulation (EU) 2016/679 in developing guidelines to specify at the technical level the conditions allowing the licit use of personal data by data controllers for IT security purposes with the objective of protecting their infrastructure by detecting and blocking attacks against their information systems in the context of: (i) Regulation (EU) 2016/679[1a]; (ii) Directive (EU) 2016/1148[1b]; and (iii) Directive 2002/58/EC[1c];
	[1a] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119,

4.5.2016, p. 1).

[1b] (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[1c] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

Justification

Establishing proper cooperation mechanisms.

Amendment 38

Proposal for a regulation
Article 5 – paragraph 1 – point 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 advice, as well as facilitating the exchange of best practices between competent authorities;	(2) the promotion of an enhanced level of security of electronic communications***, data storage and data processing***, including by providing expertise and advice, as well as facilitating the exchange of best practices between competent authorities;

Amendment 39

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

Text proposed by the Commission	*Amendment*
	2a. The Agency shall facilitate the establishment and launch of a long-term European cybersecurity project to support the growth of an independent EU

cybersecurity industry, and to mainstream cybersecurity into all EU ICT developments.

Justification

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

Amendment 40

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

Text proposed by the Commission	*Amendment*
Upon a request by ***two*** or more Member States concerned, and with the sole purpose of providing advice for the prevention of future incidents, the Agency shall provide support to or carry out an ex-post technical enquiry following notifications by affected undertakings of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148. The Agency shall also carry out such an enquiry upon a duly justified request from the Commission in agreement with the concerned Member States in case of such incidents affecting more than two Member States.	Upon a request by ***one*** or more Member States concerned, and with the sole purpose of providing advice for the prevention of future incidents, the Agency shall provide support to or carry out an ex-post technical enquiry following notifications by affected undertakings of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148. The Agency shall also carry out such an enquiry upon a duly justified request from the Commission in agreement with the concerned Member States in case of such incidents affecting more than two Member States.

Amendment 41

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

Text proposed by the Commission	*Amendment*
(a) aggregating reports from national sources with a view to contribute to establishing common situational awareness;	(a) aggregating reports from national ***and international*** sources with a view to contribute to establishing common situational awareness;

Amendment 42

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

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

Amendment 43

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

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

Amendment 44

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

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

standardised and transparent process;

Amendment 45

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

Text proposed by the Commission	*Amendment*
(b) facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products and services, as well as draw up, in collaboration with Member States, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148;	(b) ***consult the international standardisation bodies and European standardisation organisations on the development of standards, to ensure the appropriateness of standards used in European Cybersecurity certification schemes and*** facilitate the establishment and take-up of ***relevant*** European and international standards for risk management and for the security of ICT products and services, as well as draw up, in collaboration with Member States, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148;

Amendment 46

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

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

policies;

Amendment 47

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

Text proposed by the Commission	*Amendment*
	(b b) draw up guidelines on minimum security requirements for IT devices placed on the market in the Union or exported from the Union;

Amendment 48

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

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

Amendment 49

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

Text proposed by the Commission	*Amendment*
(e) raise awareness of the public about cybersecurity risks, ***and*** provide guidance on good practices for ***individual*** users aimed at citizens and organisations;	(e) raise awareness of the public about cybersecurity risks, provide guidance on good practices for users aimed at citizens and organisations ***and promote the adoption of preventive strong IT security measures and reliable data protection and privacy***;

Amendment 50

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

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

Amendment 51

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

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

Amendment 52

Proposal for a regulation
Article 13 – paragraph 1

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

Amendment 53

Proposal for a regulation

Article 14 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
e) assess and adopt the consolidated annual report on the Agency's activities and send both the report and its assessment by 1 July of the following year, to the European Parliament, the Council, the Commission and the Court of Auditors. The annual report shall include the accounts ***and*** describe how the Agency has met its performance indicators. The annual report shall be made public;	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 54

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

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

Amendment 55

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

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

Amendment 56

Proposal for a regulation
Article 19 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	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 57

Proposal for a regulation
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in the cybersecurity, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities.	1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, ***and*** providers of electronic communications networks or services available to the public, ***in particular European ICT industry and providers, associations of small and medium-sized enterprises,*** consumer groups ***and associations***, academic experts in the ***field of*** cybersecurity***, the European standardisation organisations as defined in point (8) of Article 2 of Regulation (EU) No 1025/2012, the relevant sectoral Union agencies and bodies***, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities.

Amendment 58

Proposal for a regulation
Article 20 – paragraph 4

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

Amendment 59

Proposal for a regulation
Article 20 – paragraph 5

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

Amendment 60

Proposal for a regulation
Article 20 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5 a. The Permanent Stakeholders' Group shall advise the Agency in the preparation of candidate European Cybersecurity certification schemes.

Amendment 61

Proposal for a regulation
Article 23 – paragraph 2

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

Justification

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

Amendment 62

Proposal for a regulation
Article 43 – paragraph 1

Text proposed by the Commission	*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	A European cybersecurity certification scheme shall ***be established in order to boost the level of security within the digital single market and adopt a harmonised approach, at EU level, to European certification, with a view to ensuring that ICT products, services and systems are resistant to cyber-attacks.***

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

Amendment 63

Proposal for a regulation
Article 43 a (new)

Text proposed by the Commission	*Amendment*
	Article 43 a
	Work Programme
	ENISA shall, after consulting the European Cybersecurity Certification Group and the Permanent Stakeholders' Group and after approval by the Commission, establish a work programme detailing common actions to be undertaken at Union level to ensure the consistent application of this Title, and containing a priority list of ICT products and services for which it considers a European cybersecurity certification scheme to be needed.
	The work programme shall be established not later than [six months after entry into force of this Regulation] and a new work programme shall be established every two years thereafter. The work programme shall be made publicly available.

Amendment 64

Proposal for a regulation
Article 44 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.	1. Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 ***or the Permanent Stakeholders' Group established under Article 20*** may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.

Amendment 65

Proposal for a regulation
Article 44 – paragraph 2

Text proposed by the Commission	*Amendment*
2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult ***all*** relevant stakeholders ***and*** closely cooperate with the Group***.*** The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary.	2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult ***the Permanent Stakeholders' Group, in particular the European standardisation organisations and all other*** relevant stakeholders***, including consumer organisations, in a formal, standardised and transparent process, and shall*** closely cooperate with the Group ***taking into account already existing national and international standards. When preparing each candidate scheme, ENISA shall establish a checklist of risks and corresponding cybersecurity features.*** The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary. ***Where relevant, ENISA may also set up a Stakeholder Consultation expert group, composed of members of the Permanent Stakeholders' Group and any other***

relevant stakeholders with specific expertise in the field of a given candidate scheme, in order to provide further assistance and advice.

Amendment 66

Proposal for a regulation
Article 44 – paragraph 3

Text proposed by the Commission	*Amendment*
3. ENISA shall transmit the candidate European cybersecurity certification scheme prepared in accordance with paragraph 2 of this Article to the Commission.	3. ENISA shall transmit the candidate European cybersecurity certification scheme prepared in accordance with paragraph 2 of this Article to the Commission***, which shall assess its suitability for achieving the objectives of the request referred to in paragraph 1***.

Amendment 67

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

Text proposed by the Commission	*Amendment*
	3a. ENISA shall observe professional secrecy with regard to all information obtained in carrying out its tasks under this Regulation.

Amendment 68

Proposal for a regulation
Article 44 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The Commission***, based on the candidate scheme proposed by ENISA, may*** adopt ***implementing*** acts, in accordance with Article ***55(1), providing for*** European cybersecurity certification schemes for ICT products and services	4. The Commission ***is empowered to*** adopt ***delegated*** acts, in accordance with Article ***55a, concerning the establishment of*** European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46

meeting the requirements of Articles 45, 46 and 47 of this Regulation.	and 47 of this Regulation. ***When adopting those delegated acts, the Commission shall base the cybersecurity certification schemes for ICT products and services on any relevant candidate scheme proposed by ENISA. The Commission may consult the European Data Protection Board and take account of its view before adopting such delegated acts.***

Amendment 69

Proposal for a regulation
Article 44 – paragraph 5

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

Amendment 70

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

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

Amendment 71

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

Text proposed by the Commission	*Amendment*
(g) ensure that ICT products and services are provided with ***up to date***	(g) ensure that ICT products and services are provided with ***up-to-date***

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

Amendment 72

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

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

Amendment 73

Proposal for a regulation
Article 46 – paragraph 1

Text proposed by the Commission	*Amendment*
1. ***A*** European cybersecurity certification scheme may specify one or more of the following assurance levels: ***basic, substantial and/or high***, for ICT products and services issued under that scheme.	1. ***Each*** European cybersecurity certification scheme may specify one or more of the following ***risk-based*** assurance levels: ***"functionally secure"; "substantially secure" and/or "highly secure"***, for ICT products and services issued under that scheme. ***The assurance levels for each candidate European cybersecurity certification scheme shall be identified on the basis of the risks identified in the checklist established in Article 44(2) and the availability of cybersecurity features to counter those risks in the ICT products and services to which the certification***

scheme applies.

Amendment 74

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

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

Amendment 75

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

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

Amendment 76

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

Text proposed by the Commission	*Amendment*
(a) assurance level ***basic*** shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides ***a limited*** degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto,	(a) assurance level ***"functionally secure"*** shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides ***an adequate*** degree of confidence in the claimed or asserted cybersecurity qualities of an ICT ***process,*** product or service, and is characterised with reference to technical specifications, standards and procedures

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

Amendment 77

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

Text proposed by the Commission	*Amendment*
(b) assurance level ***substantial*** shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of cybersecurity incidents;	(b) assurance level ***"substantially secure"*** shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of an ICT ***process,*** product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of cybersecurity incidents;

Amendment 78

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

Text proposed by the Commission	*Amendment*
(c) assurance level ***high*** shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service than certificates with the assurance level ***substantial***, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical	(c) assurance level ***"highly secure"*** shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT ***process,*** product or service than certificates with the assurance level ***substantially secure***, and is characterised with reference to technical specifications, standards and procedures related thereto,

controls, the purpose of which is to prevent cybersecurity incidents.	including technical controls, the purpose of which is to prevent cybersecurity incidents. ***This shall apply in particular to products and services intended for use by operators of essential services, as defined in Art 4(4) of Directive 2016/1148/EU.***

Amendment 79

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

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

Amendment 80

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

Text proposed by the Commission	*Amendment*
(a) subject-matter and scope of the certification, including the type or categories of ICT products and services covered;	(a) subject-matter and scope of the certification ***scheme***, including ***any specific sectors covered, and*** the type or categories of ICT products and services covered;

Amendment 81

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

Text proposed by the Commission	*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 and services are evaluated, ***in particular*** by reference to international***, European, or national*** standards or technical specifications;

Amendment 82

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

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

Amendment 83

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

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

Amendment 84

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

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

Amendment 85

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

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

Amendment 86

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

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

Amendment 87

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

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

Amendment 88

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

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

Amendment 89

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

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

Amendment 90

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

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

Amendment 91

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

Text proposed by the Commission	*Amendment*
	(m a) maximum period of validity of certificates;

Amendment 92

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

Text proposed by the Commission	*Amendment*
	(m b) rules concerning resistance and resilience testing for the "highly secure" assurance level.

Amendment 93

Proposal for a regulation
Article 47 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where a specific Union act so provides, certification under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that act.	3. Where a specific ***future*** Union act so provides, certification under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that act.

Amendment 94

Proposal for a regulation
Article 48 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ***The*** certification shall be voluntary, unless otherwise specified in Union law.	2. ***Certification under a European cybersecurity certification scheme shall be mandatory for ICT products and services with a high inherent risk that are specifically intended for use by operators of essential services, as defined in Article 4(4) of Directive 2016/1148/EU. For all other ICT products and services***

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

Amendment 95

Proposal for a regulation
Article 48 – paragraph 3

Text proposed by the Commission	*Amendment*
3. ***A*** European cybersecurity ***certificate*** pursuant to this Article shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44.	3. European cybersecurity ***certificates*** pursuant to this Article shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44. ***As an alternative to certification by conformity assessment bodies, product manufacturers and service providers may, where the scheme in question provides for such a possibility, make a self-declaration of conformity in which they declare that a process, product or service complies with the criteria of the certification scheme. In such cases, the product manufacturer or service provider shall, upon request, provide the self-declaration of conformity to the requesting national certification supervisory authority and ENISA.***

Amendment 96

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

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

of the following:

Amendment 97

Proposal for a regulation
Article 48 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The natural or legal person which submits its ICT products or services to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure.	5. The natural or legal person which submits its ICT products or services to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure***, including information on any known security vulnerabilities***.

Amendment 98

Proposal for a regulation
Article 48 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Certificates shall be issued for a maximum period ***of three years*** and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.	6. Certificates shall be issued ***and shall remain valid*** for a maximum period ***defined in each certification scheme*** and may be renewed, under the same conditions, provided that the relevant requirements ***of that scheme, including any revised or amended requirements,*** continue to be met.

Amendment 99

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

Text proposed by the Commission	*Amendment*
	6 a. Certificates shall remain valid for all new versions of a process, product or service, where the primary reason for the new version is to patch, fix, or otherwise

address known or potential security vulnerabilities or threats.

Amendment 100

Proposal for a regulation
Article 49 – paragraph 1

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

Amendment 101

Proposal for a regulation
Article 49 – paragraph 3

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

Amendment 102

Proposal for a regulation
Article 50 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Each national certification supervisory authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise.	3. Each national certification supervisory authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise ***and shall not be a conformity assessment body or a national accreditation body***.

Amendment 103

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

Text proposed by the Commission	*Amendment*
(a) monitor and enforce the application of the provisions under this Title at national level and supervise compliance ***of the certificates that have been issued by conformity assessment bodies established in their respective territories*** with the ***requirements set out in this Title and in the corresponding*** European cybersecurity certification ***scheme;***	(a) monitor and enforce the application of the provisions under this Title at national level and supervise compliance***, in accordance*** with the ***rules adopted by the*** European Cybersecurity Certification ***Group pursuant to point (da) of Article 53(3), of:***
	i) the certificates that have been issued by conformity assessment bodies established in their respective territories with the requirements set out in this Title and in the corresponding European cybersecurity certification scheme; and
	ii) self-declarations of conformity made under a scheme for an ICT process, product or service;

Amendment 104

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

Text proposed by the Commission	*Amendment*
(b) monitor ***and*** supervise the activities of conformity assessment bodies for the purpose of this Regulation, including in	(b) monitor***,*** supervise ***and, at least every two years, assess*** the activities of conformity assessment bodies for the

relation to the notification of conformity assessment bodies and the related tasks set out in Article 52 of this Regulation;	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 105

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-declarations of conformity made***, investigate, to the extent appropriate, the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation within a reasonable time period;

Amendment 106

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

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

Amendment 107

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

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

other public authorities, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;	***national accreditation bodies*** or other public authorities, including by sharing information on possible non-compliance***, including deceptive, false, or fraudulent claims of certification,*** of ICT products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;

Amendment 108

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

Text proposed by the Commission	*Amendment*
	(c a) to revoke the accreditation of conformity assessment bodies that do not comply with this Regulation;

Amendment 109

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

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

Amendment 110

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

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

Amendment 111

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

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

Amendment 112

Proposal for a regulation
Article 50 a (new)

Text proposed by the Commission	*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 of this Regulation.
	2. Peer review shall cover the assessments of the procedures put in place by national certification supervisory authorities, in particular the procedures for checking the compliance of the products that are subject to cybersecurity certification, the competence of the personnel, the correctness of the checks and the inspection methodology as well as the correctness of the results. Peer review shall also assess whether national certification supervisory authorities in question have sufficient resources for the proper performance of their duties as required by Article 50(4).
	3. Peer review of a national certification supervisory authority shall be carried out by two national certification supervisory authorities of other Member

States and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review and shall decide on its participation on the basis of a risk assessment analysis.

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

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

Amendment 113

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

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

Amendment 114

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

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

Amendment 115

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

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

Amendment 116

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

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

Amendment 117

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

Text proposed by the Commission	*Amendment*
	(f b) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards and, where appropriate, recommend areas to ENISA in which it should engage with relevant international and European standardisation organisations to address insufficiencies or gaps in internationally recognised standards;

Amendment 118

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

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

Amendment 119

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

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

Amendment 120

Proposal for a regulation
Article 55 a (new)

Text proposed by the Commission	*Amendment*
	Article 55a
	Exercise of the delegation
	The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
	The power to adopt delegated acts referred to in Articles 44(4) and 50a(4) shall be conferred on the Commission for a period of 5 years from [date of entry into force of the basic legislative act]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the 5 year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.
	The delegation of power referred to in Articles 44(4) and 50a(4)may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
	Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.
	As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
	A delegated act adopted pursuant to Article 44(4) or 50a(4) shall enter into

force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')
References	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Committee responsible Date announced in plenary	ITRE 23.10.2017
Opinion by Date announced in plenary	IMCO 23.10.2017
Associated committees - date announced in plenary	18.1.2018
Rapporteur Date appointed	Nicola Danti 25.9.2017
Discussed in committee	21.2.2018 21.3.2018
Date adopted	17.5.2018
Result of final vote	+: 31 –: 2 0: 1
Members present for the final vote	John Stuart Agnew, Pascal Arimont, Dita Charanzová, Carlos Coelho, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Dennis de Jong, Pascal Durand, Evelyne Gebhardt, Robert Jarosław Iwaszkiewicz, Liisa Jaakonsaari, Marlene Mizzi, Nosheena Mobarik, Jiří Pospíšil, Andreas Schwab, Olga Sehnalová, Jasenko Selimovic, Ivan Štefanec, Catherine Stihler, Mylène Troszczynski, Mihai Ţurcanu, Anneleen Van Bossuyt, Marco Zullo
Substitutes present for the final vote	Jan Philipp Albrecht, Kaja Kallas, Arndt Kohn, Emma McClarkin, Adam Szejnfeld, Marc Tarabella, Lambert van Nistelrooij, Kerstin Westphal
Substitutes under Rule 200(2) present for the final vote	Inés Ayala Sender, Flavio Zanonato

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

31	+
ALDE	Dita Charanzová, Kaja Kallas, Jasenko Selimovic
ECR	Daniel Dalton, Emma McClarkin, Nosheena Mobarik, Anneleen Van Bossuyt
EFDD	Marco Zullo
GUE/NGL	Dennis de Jong
PPE	Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Jiří Pospíšil, Andreas Schwab, Ivan Štefanec, Adam Szejnfeld, Mihai Ţurcanu, Lambert van Nistelrooij
S&D	Inés Ayala Sender, Nicola Danti, Evelyne Gebhardt, Liisa Jaakonsaari, Arndt Kohn, Marlene Mizzi, Olga Sehnalová, Catherine Stihler, Marc Tarabella, Kerstin Westphal, Flavio Zanonato
Verts/ALE	Jan Philipp Albrecht, Pascal Durand

2	-
EFDD	John Stuart Agnew, Robert Jarosław Iwaszkiewicz

1	0
ENF	Mylène Troszczynski

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

16.5.2018

OPINION OF THE COMMITTEE ON BUDGETS

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Rapporteur for opinion: Jens Geier

SHORT JUSTIFICATION

The Rapporteur welcomes in general the Commission proposal for a "Cybersecurity Act" to further enhance the role of the European Agency for Network and Information Security (ENISA), as the issue of cybersecurity is clearly cross-border and a more European approach is appropriate. The Rapporteur particularly welcomes the proposal of the Commission to provide a permanent mandate to ENISA, given its increased role and for providing certainty for staff members of the agency. The Commission proposes an increase of AD/AST staff by 41 posts by 2022[1] and an increase of the annual budget of the agency up to EUR 23 million in 2022[2].

The Rapporteur is of the opinion that the current arrangement of the seat, namely the multiple locations of the agency in Heraklion and Athens, hinder the efficient functioning in fulfilling the mandate of the agency. The Inter-institutional Working Group on agencies' resources, as established following the agreement on the budget 2014, recommends "the Commission to carry out an evaluation of multiple locations of agencies (double seats, existence of technical sites in addition to the seat, local offices and secondment of staff outside headquarters) based on a consistent approach and using clear and transparent criteria, in particular with a view to assessing their added value, also in light of the costs incurred". All EU institutions agreed to this recommendation, and the Rapporteur believes that such an evaluation should be carried out swiftly. Following such an evaluation, the institutions should draw the necessary conclusions without further delay.

The Rapporteur further believes that the mandate of the agency in providing expertise could be further strengthened by providing the agency with a budget for commissioning its own budget for research and development activities. For such a budget, the agency should be

[1] It includes 26 AD, 6 AST and 9 Seconded National Experts. It does not include estimated requirements for the parent Directorate General, contractual agents and external contractors.
[2] As estimate, without prejudice of the EU funding after 2020.

equipped with the necessary resources.

Further savings could be generated by allowing the agency to receive translation services from other service providers. The democratic oversight of the agency could be strengthened by nominating a representative of the European Parliament to the Management Board, as in line with the Common Approach on Agencies.

AMENDMENTS

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

Amendment 1

Proposal for a regulation
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3 a) ENISA should give more practical and information based support to the EU 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 form external sources and to creating a strategic supply chain inside the Union.

Amendment 2

Proposal for a regulation
Recital 4

Text proposed by the Commission	*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 defences. However, while cyber-attacks are often cross-border, policy responses by cybersecurity authorities and law enforcement competences are	(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.

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 3

Proposal for a regulation
Recital 10

Text proposed by the Commission	*Amendment*
(10) Within the framework of Decision 2004/97/EC, Euratom, adopted at the meeting of the European Council on 13 December 2003, the representatives of the Member States decided that ENISA would have its seat in a town in Greece to be determined by the Greek Government. The Agency's host Member State should ensure the best possible conditions for the smooth and efficient operation of the Agency. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and to enhance the efficiency of networking activities that the Agency be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of the	(10) Within the framework of Decision 2004/97/EC, Euratom, adopted at the meeting of the European Council on 13 December 2003, the representatives of the Member States decided that ENISA would have its seat in a town in Greece to be determined by the Greek Government. The Agency's host Member State should ensure the best possible conditions for the smooth and efficient operation of the Agency. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and to enhance the efficiency of networking activities that the Agency be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of the

Agency. The necessary arrangements should be laid down in an agreement between the Agency and the host Member State concluded after obtaining the approval of the Management Board of the Agency.	Agency. The necessary arrangements should be laid down in an agreement between the Agency and the host Member State concluded after obtaining the approval of the Management Board of the Agency. ***That agreement should be revised following the evaluation carried out by the Commission as recommended by the Inter-institutional Working Group on agencies' resources with a view of increasing the efficiency of the Agency and the location of the Agency should be reviewed.***

Amendment 4

Proposal for a regulation
Recital 12

Text proposed by the Commission	*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. 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.	(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 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 5

Proposal for a regulation
Recital 15 a (new)

Text proposed by the Commission	*Amendment*
	(15 a) International law applies to cyberspace and the 2013 and 2015 UN Group of Governmental Experts on Information Security (UNGGE) reports provide relevant guidelines, in particular as regards the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules. The relevance of the Tallinn Manual 2.0 in this context is an excellent basis for a debate on how international law applies to cyberspace and it is now time for the Member States to start analysing and applying the Manual.

Amendment 6

Proposal for a regulation
Recital 36

Text proposed by the Commission	*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.	(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. ***The Agency should be attributed an additional budget for research and development activities complementary to existing Union research programmes.***

Amendment 7

Proposal for a regulation

Recital 46 a (new)

Text proposed by the Commission	*Amendment*
	(46 a) The Agency's budget should be prepared in accordance with the principle of performance-based budgeting, taking into account the Agency's objectives and the expected results of its tasks.

Amendment 8

Proposal for a regulation
Article 4 – paragraph 4

Text proposed by the Commission	*Amendment*
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.	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 ***in order to achieve coordination and financial savings, to avoid duplication and to promote synergy and complementarity as regards their activities***.

Amendment 9

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

Text proposed by the Commission	*Amendment*
	(g a) publish and promote its activities and the results of its work in order to increase visibility and awareness among citizens.

Amendment 10

Proposal for a regulation
Article 10 –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 11

Proposal for a regulation
Article 13 – paragraph 1

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

Amendment 12

Proposal for a regulation
Article 26 – paragraph 1 – subparagraph 1 (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(1) 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 13

Proposal for a regulation
Article 36 – paragraph 5

Text proposed by the Commission	*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.	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 14

Proposal for a regulation
Article 37 – paragraph 2

Text proposed by the Commission	*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.	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 15

Proposal for a regulation
Article 41 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	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 16

Proposal for a regulation
Article 41 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. Following the Commission's evaluation as recommended by the Inter-institutional Working Group on agencies' resources, the Headquarters Agreement of the Agency shall be revised and the Agency's location shall be reviewed accordingly.

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')
References	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Committee responsible Date announced in plenary	ITRE 23.10.2017
Opinion by Date announced in plenary	BUDG 23.10.2017
Rapporteur Date appointed	Jens Geier 26.9.2017
Discussed in committee	21.3.2018
Date adopted	16.5.2018
Result of final vote	+: 22 –: 4 0: 0
Members present for the final vote	Nedzhmi Ali, Jean Arthuis, Reimer Böge, Lefteris Christoforou, Gérard Deprez, Manuel dos Santos, André Elissen, José Manuel Fernandes, Eider Gardiazabal Rubial, Jens Geier, Esteban González Pons, Ingeborg Gräßle, Iris Hoffmann, John Howarth, Bernd Kölmel, Vladimír Maňka, Liadh Ní Riada, Jan Olbrycht, Răzvan Popa, Jordi Solé, Isabelle Thomas, Inese Vaidere, Marco Zanni, Stanisław Żółtek
Substitutes present for the final vote	Ivana Maletić, Andrey Novakov

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

22	+
ALDE	Nedzhmi Ali, Jean Arthuis, Gérard Deprez
ECR	Bernd Kölmel
PPE	Reimer Böge, Lefteris Christoforou, José Manuel Fernandes, Esteban González Pons, Ingeborg Gräßle, Ivana Maletić, Andrey Novakov, Jan Olbrycht, Inese Vaidere
S&D	Eider Gardiazabal Rubial, Jens Geier, Iris Hoffmann, John Howarth, Vladimír Maňka, Răzvan Popa, Isabelle Thomas, Manuel dos Santos
Verts/ALE	Jordi Solé

4	-
ENF	André Elissen, Marco Zanni, Stanisław Żółtek
GUE/NGL	Liadh Ní Riada

0	0

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

16.3.2018

OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Rapporteur: Jan Philipp Albrecht

SHORT JUSTIFICATION

The Rapporteur welcomes the Commission's proposal for a "Cybersecurity Act"[1], as it better defines the role of ENISA in the changed IT security ecosystem and develops measures on IT security standards, certification and labelling to make ICT-based systems, including connected objects, more secure.

Still, the Rapporteur considers that further improvements could be made. The Rapporteur firmly believes that information security is paramount to the protection of fundamental rights of citizens as enshrined in the Charter of Fundamental Rights of the EU, as well as the fight against cybercrime and the protection of democracy and the rule of law.

Fundamental rights: Insecure systems may lead to data breaches or identity fraud that could cause real harm and distress to individuals, including a risk to their lives, their privacy, their dignity, or their property. For example, witnesses may be at risk of intimidation and physical harm or women may be at risk of domestic violence, if their home addresses are disclosed. For the internet of things that also contains physical actuators and not just sensors, the physical integrity and life of individuals may be at risk due to attacks against information systems, The amendments proposed by the Rapporteur focus in particular on the protection of Articles 1, 2, 3, 6, 7, 8, 11 and 17 of the Charter of Fundamental Rights of the EU. There is even emerging constitutional case law that derives a special "fundamental right to the confidentiality and integrity of information-technical systems"[2] from general personality rights, as adapted to the current digital world.

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final/2.
[2] German Constitutional Court, Judgement of 27 February 2008, cases 1 BvR 370/07, 1 BvR 595/07.

Fight against cybercrime: Some forms of crimes committed online, such as phishing attacks or financial and banking fraud, consist of abuse of trust, which cannot be countered by IT security measures - against these forms of crimes, the Rapporteur welcomes the proposed regular outreach and public education campaigns directed to end-users, organised by ENISA. Other forms of online crimes involve attacks against information systems such as hacking or distributed denial of service (DDoS) attacks - against these forms of crimes, the Rapporteur believes that reinforcing IT security will effectively strengthen the fight against and especially the prevention of cybercrime.

Democracy and the rule of law: Attacks against IT systems from governments and non-state actors pose a clear and increasing threat to democracy through their interference in free and fair elections, for example by manipulating facts and opinions influencing how citizens will vote, interfering with the voting process and changing the results of the vote or undermining confidence in the integrity of the vote.

The Rapporteur therefore proposes, in his draft LIBE Opinion, to amend the Commission proposal focussing on the following key LIBE issues:

- The Agency should play a stronger role in promoting adoption by all actors of the European Information Society of preventive strong privacy enhancing technologies and IT security measures;

- The Agency should propose policies establishing clear responsibilities and liabilities for all stakeholders taking part in ICT eco-systems where the failure to act with proper IT security due diligence could result in severe safety impacts, massive destructions in the environment, trigger a systemic financial or economic crisis;

- The Agency should propose clear and mandatory baseline IT security requirements, in consultation with IT security experts;

- The Agency should propose an IT security certification scheme allowing ICT vendors to increase the transparency for the consumer about upgradability and software support time. Such a certification scheme needs to be dynamic as security is a process that needs constant improvement;

- The Agency should make it easier and cheaper for manufacturers of ICT products to implement Security by Design principles by releasing guidelines and best practices;

- The Agency should, upon invitation of Union institutions, bodies, offices and agencies as well as Member States, conduct regular preventive IT security audits of their critical infrastructures (Right to Audit);

- The Agency should immediately report IT security vulnerabilities that are not yet publicly known to manufacturers. The Agency should not conceal or exploit undisclosed vulnerabilities in companies and products for its own purposes. By developing, buying up and exploiting back doors in IT systems with taxpayers' money, government bodies are putting the security of citizens at risk. In order to protect other stakeholders who deal responsibly with such vulnerabilities, the Agency should propose policies for the responsible exchange of information on “Zero days” and other

types of security vulnerabilities that are not yet publicly known and that facilitate the closing of vulnerabilities;

- To allow the EU to catch up with IT security industries in third countries, the Agency should identify and initiate the launch of a long term EU-IT security project of a scope comparable to what has been done for the aviation industry with Airbus;

The Commission proposal should avoid using the term “cybersecurity” as it is legally vague and could lead to uncertainties. Instead, the Rapporteur proposes to replace “cybersecurity” with “IT security” to improve legal certainty

AMENDMENTS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a regulation
Title

Text proposed by the Commission	*Amendment*
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on ENISA, the "***EU Cybersecurity*** Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology ***cybersecurity*** certification ("Cybersecurity Act")	on ENISA, the "***European Network and Information Security*** Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology ***IT security*** certification ("***IT Security*** Act")
	(This amendment applies throughout the text.)

Justification

The prefix “cyber”, derived from 1960s science-fiction works, has been increasingly used to describe the negative aspects of the Internet (cyberattack, cybercrime, etc.) but is legally very vague. The Rapporteur proposes changing the term “cybersecurity” to “IT security” for legal certainty.

Amendment 2

Proposal for a regulation
Recital 2

Text proposed by the Commission	*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.	(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 ***IT security***. In this context, the limited ***and fragmented*** use of certification leads to insufficient information for ***organisations*** and individual users about the ***IT security*** features of ICT products and services, undermining trust in digital solutions. ***ICT networks provide the backbone for digital products and services which have the potential to support all aspects of citizens' lives and drive Europe's economic growth. To ensure that the objectives of the digital single market are fully achieved, the essential technological building blocks on which important areas such as e-health, IoT, artificial intelligence, quantum technology as well as intelligent transport systems and advanced manufacturing rely, must be in place.***

Amendment 3

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) Cyber-attacks are on the increase and a connected economy and society that	(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

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 ***IT security*** 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 ***IT security*** 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

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) In light of the increased ***cybersecurity*** challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens	(5) In light of the increased ***IT security*** 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 ***deliver a coordinated EU response and*** increase awareness of

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.

citizens and businesses on ***IT security*** 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 ***IT security*** requirements and evaluation criteria across national markets and sectors. ***Alongside Union-wide certification, there is a range of voluntary measures widely accepted in the market place, depending on the product, service, use or standard. These measures as well as the industry bottom up approach, including the use of security-by-design, leveraging and contributing to international standards, should be encouraged.***

Amendment 5

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) The Union has already taken important steps to ensure ***cybersecurity*** and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to ***cybersecurity*** threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of ***cybersecurity***, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). The NIS Directive ***put*** in place requirements concerning national capabilities in the area of ***cybersecurity***, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for economy and	(7) The Union has already taken important steps to ensure ***IT security*** and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to ***IT security*** threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of ***IT security***, 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 ***fulfils the digital single market strategy and together with other instruments, such as Directive .../... [establishing the European Electronic Communications Code], Regulation (EU) 2016/679 of the European Parliament and of the Council[1a] and Directive 2002/58/EC of the European Parliament and of the***

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***.

Council[1b], puts in place requirements concerning national capabilities in the area of ***IT security***, 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 ***IT security***.

[1a] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1)

[1b] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Amendment 6

Proposal for a regulation
Recital 8

Text proposed by the Commission	*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 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.	(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 ***IT security*** policy, it is necessary to review the mandate of ENISA to define its role in the changed ***IT security*** ecosystem and ensure it ***undertakes a leading role which will*** effectively ***improve*** the Union's response to ***IT security*** 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 7

Proposal for a regulation
Recital 11

Text proposed by the Commission	*Amendment*
(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.	(11) Given the increasing ***IT security*** 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. ***Due regard should be given to further enhancement of capacity of the Agency.***

Justification

It is essential that we undue the lack of capacity of the agency. We must also strive towards establishing the further development of the agency given how critically important cyber security is today and more importantly how important it will be ´tomorrow´. Note the Russian interference in election, increasing capacities of superpowers and states around the world, imminent digitalisation of major sectors.

Amendment 8

Proposal for a regulation

Recital 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) The challenges in the field of IT security are, in the digital age, often closely interlinked with challenges in the field of data protection, the protection of private life and the protection of electronic communications. In order for the agency to be able to address those challenges appropriately, there is a need for close cooperation and frequent consultation with the bodies established under Regulation (EC) 45/2001of the European Parliament and of the Council[1a], Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EC) No 1211/2009 as well as with industry and civil society.
	[1a] Regulation (EC) 45/2001of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Amendment 9

Proposal for a regulation
Recital 12

Text proposed by the Commission	*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	(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.	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 ***clear agenda and a*** set of tasks ***and objectives which*** the Agency is to accomplish ***should be clearly defined*** 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 10

Proposal for a regulation
Recital 14

Text proposed by the Commission	*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, 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.	(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***, 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 ***IT security*** threat landscape, it is clear that Member States must be supported by more comprehensive, cross-policy approach to building cyber resilience.

Amendment 11

Proposal for a regulation
Recital 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) The Commission should propose

	the introduction of mandatory cooperation between Member States concerning the protection of critical information infrastructure.

Amendment 12

Proposal for a regulation
Recital 26

Text proposed by the Commission	*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. 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.	(26) To understand better the challenges in the field of ***IT security***, 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 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 ***IT security***. The Agency should furthermore support Member States and Union institutions, agencies and bodies in identifying emerging trends and preventing problems related to ***IT security***, by performing analyses of threats***,*** incidents ***and vulnerabilities***.

Amendment 13

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) The Agency should contribute towards raising the awareness of the public about risks related to ***cybersecurity*** and provide guidance on good practices for	(28) The Agency should contribute towards raising the awareness of the public about risks related to ***IT security*** and provide guidance on good practices for

individual users aimed at citizens and organisations. The Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing ***publicly*** available information regarding significant incidents**,** and by compiling reports with a view to providing guidance to businesses ***and*** citizens and ***improving the overall*** level ***of preparedness and resilience***. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users***, aiming at promoting*** safer individual online behaviour and ***raising*** awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as ***promoting*** basic authentication ***and data protection advice***. The Agency should play a central role in accelerating end-user awareness on security of devices.	individual users aimed at citizens and organisations. ***To improve the overall level of preparedness and resilience,*** the Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing available information regarding significant incidents and by compiling reports with a view to providing guidance to businesses**,** citizens and ***relevant authorities at Union and national*** level. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users***. These campaigns should promote IT security education and*** safer individual online behaviour and ***raise*** awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, ***forgery and illegal content,*** as well as ***advocating data protection and*** basic authentication ***to prevent data and identity theft***. The Agency should play a central role in accelerating end-user awareness on security of devices.

Amendment 14

Proposal for a regulation
Recital 28 a (new)

Text proposed by the Commission	*Amendment*
	(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 15

Proposal for a regulation
Recital 30

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

Justification

As there are cybersecurity issues in Galileo, especially in ground segments, the cooperation with Global Navigation Satellite Systems Agency actually strengthens the role of ENISA, while enhancing, at the same time, the credibility of Galileo.

Amendment 16

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) The Agency should encourage Member States and service providers to	(35) The Agency should encourage Member States***, hardware and software***

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.

manufacturers and ICT and on-line service providers to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal ***IT security***. In particular, service providers and product manufacturers should withdraw or recycle products and services that do not meet ***IT security*** standards. In cooperation with competent authorities, ENISA may disseminate information regarding the level of ***IT security*** of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the ***IT*** security of their products and services. ***The Agency should work with stakeholders to develop a Union-wide approach to the responsible disclosure of vulnerabilities and should promote best practice in this area.***

Amendment 17

Proposal for a regulation
Recital 44

Text proposed by the Commission	*Amendment*
(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, 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.	(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. ***Given the importance of certification requirements to ensure trust in IoT, the Commission should***

	specifically consider implementing measures to ensure Union-wide harmonisation of security standards for IoT devices.

Amendment 18

Proposal for a regulation
Recital 50

Text proposed by the Commission	*Amendment*
(50) Currently, the ***cybersecurity*** certification of ICT products and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In this context, a certificate issued by one national ***IT security*** 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.	(50) Currently, the ***IT security*** 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 ***IT security*** 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***, and these procedures may entail additional costs for companies***. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach with regard to horizontal ***IT security*** issues, for instance in the field of the Internet of Things. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual utilisation. ***A case-by-case approach should ensure that services and products are subject to appropriate certification schemes. Additionally, a risk-based approach is needed for effective identification and mitigation of risks and to avoid increased costs for manufacturers.***

Amendment 19

Proposal for a regulation
Recital 52

Text proposed by the Commission	*Amendment*
(52) In view of the above, it is necessary to establish a European ***cybersecurity*** certification framework laying down the main horizontal requirements for European ***cybersecurity*** certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping national ***cybersecurity*** certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should be non-discriminatory and based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.	(52) In view of the above, it is necessary to establish a ***harmonised*** European ***IT security*** certification framework laying down the main horizontal requirements for European ***IT security*** 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 ***IT security*** 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 20

Proposal for a regulation
Recital 55

Text proposed by the Commission	*Amendment*
(55) The purpose of European ***cybersecurity*** certification schemes should be to ensure that ICT products and services certified under such a scheme comply with specified requirements. Such requirements concern the ability to resist, at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes,	(55) The purpose of European ***IT security*** 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.

services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the ***IT security*** requirements relating to all ICT products and services. ICT products and services and related ***IT security*** needs are so diverse***, as is their lifecycle,*** that it is very difficult to come up with general ***IT security*** requirements valid across the board. It is, therefore necessary to adopt a broad and general notion of ***IT security*** for the purpose of certification, complemented by a set of specific ***IT security*** objectives that need to be taken into account when designing European ***IT security*** 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 ***in close consultation with the Member States and industrial stakeholders***, for example by reference to standards or technical specifications. ***The individual certification schemes should be designed in such a way that all actors involved in the development of relevant IT products and services are encouraged to develop and adopt standards, norms and principles which ensure the highest possible level of security throughout the lifecycle.***

Amendment 21

Proposal for a regulation
Recital 55 a (new)

Text proposed by the Commission	*Amendment*
	(55a) ENISA should develop a certification scheme with a global perspective in order to prevent future trade barriers. In the process of developing the criteria for the certification scheme ENISA should engage in dialogue with relevant partners in the sector to

ensure market feasibility.

Amendment 22

Proposal for a regulation
Recital 56

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

Amendment 23

Proposal for a regulation
Recital 57

Text proposed by the Commission	*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 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.	(57) Recourse to European ***IT security*** certification should remain voluntary, unless otherwise provided in Union or national legislation. ***After this initial stage, and depending on the maturity of implementation in the Member States and the criticality of a product or service, potentially mandatory certification schemes for certain ICT products and services may be introduced in a phased approach for future generations of technology and in response to the policy objectives of tomorrow.*** However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national ***IT security*** certification schemes or procedures for the ICT products and services covered by a European ***IT security*** 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 ***IT security*** certification schemes for ICT products and services already covered by an existing European ***IT security*** certification scheme.

Amendment 24

Proposal for a regulation
Recital 58 a (new)

Text proposed by the Commission	*Amendment*
	(58a) Clear baseline IT security requirements should be devised by the Agency, and should be proposed to the Commission as implementing acts if appropriate, for all IT devices sold in or exported from the Union. Those requirements should be revised every two years thereafter, in order to ensure ongoing improvements. Those baseline IT

	security requirements should require, inter alia, that devices not contain any known exploitable security vulnerability, that they be capable of accepting trusted security updates, that the vendor notify the competent authorities of known vulnerabilities and repair or replace affected devices up until the time a manufacturer has made clear that security support for such devices will end.

Amendment 25

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

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

Justification

Purely linguistic amendment, removing the pleonasm present in the COM text.

Amendment 26

Proposal for a regulation
Article 2 – paragraph 1 – point 8

Text proposed by the Commission	*Amendment*
(8) ‘cyber threat’ means any potential circumstance or event that may adversely impact network and information systems, their users and affected persons.	(8) ‘cyber threat’ means any potential circumstance***, capability*** or event that may adversely impact network and information systems, their users and affected persons.

Justification

Adding important aspect, especially as regards threat assessment.

Amendment 27

Proposal for a regulation
Article 4 – paragraph 3 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	The Agency shall seek to identify critical vulnerabilities of the Union's IT security network as a whole as well as those of individual Member States. In case the Agency deems it necessary such vulnerabilities should be reported to the European Parliament.

Amendment 28

Proposal for a regulation
Article 4 – paragraph 5

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

Amendment 29

Proposal for a regulation
Article 4 – paragraph 6

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

market.	strengthen trust in the digital internal market.

Amendment 30

Proposal for a regulation
Article 4 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Agency shall promote a high level of awareness ***of citizens and businesses*** on issues related to the ***cybersecurity***.	7. The Agency shall promote a high level of awareness on issues related to the ***IT security***.

Justification

Awareness should not only be promoted towards citizens and businesses, but to all relevant actors in society, including authorities and lawmakers. This amendment deliberately leaves open the addressees of this kind of activity.

Amendment 31

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

Text proposed by the Commission	*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;	2. assisting Member States to implement consistently the Union policy and law regarding ***IT security*** notably in relation to Directive (EU) 2016/1148***, 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 risk management, incident reporting and information sharing, as well as facilitating the exchange of best practices between competent authorities in this regard;

Amendment 32

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

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

Amendment 33

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

Text proposed by the Commission	*Amendment*
	2b. proposing guidelines with the objective of ensuring that ICT vendors act with due diligence to ensure the timely fixing of IT security vulnerabilities in their products and services in order to avoid any exposure of users to cyber threats;

Amendment 34

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

Text proposed by the Commission	*Amendment*
	2c. proposing guidelines establishing a strong responsibility and liability for all stakeholders (including end-users) taking part in ICT eco-systems;

Amendment 35

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

Text proposed by the Commission	*Amendment*
	2d. proposing guidelines, in accordance with national law, regarding the responsibilities of operators of critical network infrastructures in the case of an attack against their information systems affecting their users due to a lack of due diligence by some of the users or by the operator itself, where the operator has failed to take reasonable action to prevent the incident or to mitigate its effects on all users;

Amendment 36

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

Text proposed by the Commission	*Amendment*
	2e. proposing guidelines to limit the purchase and use of "Zero days" by public authorities with the purpose of attacking information systems; promoting software audits and financing expert staff;

Amendment 37

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

Text proposed by the Commission	*Amendment*
	2f. proposing guidelines for public authorities, private companies, researchers, universities and other stakeholders to publish all critical security vulnerabilities that are not yet publicly known within the framework of a responsible disclosure;

Amendment 38

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

Text proposed by the Commission	*Amendment*
	2g. proposing guidelines for the extension of the use of "verifiable open-source code" for IT solutions in the public sector as well as for the related use of automated tools to ease review of source code and to easily verify the absence of backdoors and other possible security vulnerabilities;

Amendment 39

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

Text proposed by the Commission	*Amendment*
	(fa) and cooperate with national data protection supervisory authorities, where necessary;

Amendment 40

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

Text proposed by the Commission	*Amendment*
	2a. The Agency shall facilitate the establishment and launch of a long-term European IT security project to support the growth of an independent EU IT security industry, and to mainstream IT security into all EU IT developments.

Justification

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

Amendment 41

Proposal for a regulation
Article 7 – paragraph 5

Text proposed by the Commission	*Amendment*
5. 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.	5. Upon a request by ***a*** Member ***State***, 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.
The scope of the enquiry and the procedure to be followed in conducting such enquiry shall be agreed by the concerned Member	The scope of the enquiry and the procedure to be followed in conducting such enquiry shall be agreed by the concerned Member

States and the Agency and is without prejudice to any on-going criminal investigation concerning the same incident. The enquiry shall be concluded by a final technical report compiled by the Agency in particular on the basis of information and comments provided by the concerned Member States and undertaking(s) and agreed with the concerned Member States. A summary of the report focussing on the recommendations for the prevention of future incidents will be shared with the CSIRTs network.

States and the Agency and is without prejudice to any on-going criminal investigation concerning the same incident ***or to Member States' national security measures***. The enquiry shall be concluded by a final technical report compiled by the Agency in particular on the basis of information and comments provided by the concerned Member States and undertaking(s) and agreed with the concerned Member States. A summary of the report focussing on the recommendations for the prevention of future incidents will be shared with the CSIRTs network.

Amendment 42

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

Text proposed by the Commission	*Amendment*
	8a. The Agency shall conduct, upon the request of a Union institution, body, office or agency or of a Member State, regular independent IT security audits of critical infrastructures with the objective of identifying possible recommendations to strengthen their resilience.

Justification

ENISA should be empowered to conduct preventive IT security audit of any critical infrastructure of Member States' authorities or EU institutions, agencies, etc.)

Amendment 43

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	(1) preparing candidate European ***IT security*** certification schemes for ICT products and services in ***cooperation with***

Article 44 of this Regulation;	***industry and in*** accordance with Article 44 of this Regulation;

Justification

In this field the cooperation with industry is important.

Amendment 44

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

Text proposed by the Commission	*Amendment*
	(ca) put in place certification schemes deterring the implementation by ICT vendors and service providers of secret backdoors intentionally weakening the IT security of commercial products and services and having a detrimental impact on the global security of the internet.

Justification

This should be recognised as one of the main objectives of the Certification schemes.

Amendment 45

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

Text proposed by the Commission	*Amendment*
(d) pool, organise and make available to the public, through a dedicated portal, information on ***cybersecurity***, provided by the Union institutions, agencies and bodies;	(d) pool, organise and make available to the public, through a dedicated portal, information on ***IT security***, provided by the Union institutions, agencies and bodies ***and made available by Member States and public and private stakeholders***;

Amendment 46

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

Text proposed by the Commission	*Amendment*
(e) raise awareness of the public about ***cybersecurity*** risks, and provide guidance on good practices for individual users aimed at citizens and organisations;	(e) raise awareness of the public about ***IT security*** risks***, disseminate adequate measures for prevention of incidents***, and provide guidance on good practices for individual users aimed at citizens and organisations;

Amendment 47

Proposal for a regulation
Article 9 – paragraph 1 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) create a network of national education points of contact to support better coordination and exchange of best practices among Member States on IT security education and awareness;

Amendment 48

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

Text proposed by the Commission	*Amendment*
(g) organise, in cooperation with the Member States and Union institutions, bodies, offices ***and*** agencies regular outreach campaigns to increase ***cybersecurity*** and its visibility in the Union***.***	(g) organise, in cooperation with the Member States and Union institutions, bodies, offices***,*** agencies ***and other relevant stakeholders,*** regular outreach campaigns to increase ***IT security*** and its visibility in the Union***;***

Amendment 49

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

Text proposed by the Commission	*Amendment*
	(ga) promote the widespread adoption by all actors on the EU Digital Single

Market of preventive strong IT security measures and reliable privacy enhancing technologies as the first line of defence against attacks against information systems.

Justification

Based on the EDPS opinion (for PETs). The role of ENISA should clearly extend beyond support to Member States, the EC and EU agencies, but should also be more visible in the industry and in the general public.

Amendment 50

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

Text proposed by the Commission	*Amendment*
(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;	(a) advise the Union and the Member States on research needs and priorities in the ***areas*** of ***IT security and 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 51

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

Text proposed by the Commission	*Amendment*
(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;	(m) appoint the Executive Director ***through selection procedure 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 52

Proposal for a regulation
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in the ***cybersecurity***, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities.	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, ***the European standardisation organisations,*** academic experts in the ***IT security***, 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 53

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 54

Proposal for a regulation
Article 44 – paragraph 2

Text proposed by the Commission	*Amendment*
2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant	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.	stakeholders and closely cooperate with the Group ***and the Permanent Stakeholders' Group. The Group and the Permanent Stakeholders'*** Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary. ***Where relevant, ENISA may in addition set up a certification stakeholder working group, composed of members of the Permanent Stakeholders' Group and any other relevant stakeholders, to provide expert advice on areas covered by a specific candidate scheme.***

Justification

Industry should be involved in the drafting and preparation of candidate schemes, through a consultation process in order to provide expertise to ensure their efficient design.

Amendment 55

Proposal for a regulation
Article 44 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European ***cybersecurity*** certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.	4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European ***IT security*** certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation. ***The Commission may consult the European Data Protection Board and take account of its view before adopting such implementing acts.***

Justification

Based on the EDPS opinion. This amendment ensures consistency between certifications under the European Cybersecurity Certification Framework and under the GDPR.

Amendment 56

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

Text proposed by the Commission	*Amendment*
2. The assurance levels basic, substantial and high shall ***meet the following criteria respectively:***	2. The assurance levels basic, substantial and high shall ***refer to a certificate issued in the context of a European IT security certification scheme, which provides a corresponding degree of confidence in the claimed or asserted IT security qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related to those standards, including technical controls, the purpose of which is to decrease the risk of IT security incidents.***

Amendment 57

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

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

Amendment 58

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

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

Amendment 59

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

Text proposed by the Commission	*Amendment*
(c) assurance level high shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service than certificates with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity incidents.	***deleted***

Amendment 60

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

Text proposed by the Commission	*Amendment*
	(aa) the conformity assessment and auditing bodies;

Amendment 61

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

Text proposed by the Commission	*Amendment*
(l) identification of national ***cybersecurity*** certification schemes covering the same type or categories of ICT products and services;	(l) identification of national ***IT security*** certification schemes***, pursuant to Article 49,*** covering the same type or categories of ICT products and services;

Amendment 62

Proposal for a regulation
Article 48 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Certificates shall be issued for a maximum period of three years and may be renewed***, under the same conditions,*** provided that the relevant requirements continue to be met.	6. Certificates shall be issued for a maximum period ***determined on a case by case basis for each scheme but which shall not exceed five years*** and may be renewed provided that the relevant requirements continue to be met.

Amendment 63

Proposal for a regulation
Article 48 a (new)

Text proposed by the Commission	*Amendment*
	Article 48a
	Baseline IT security requirements
	1. The Agency shall, based on its experience with the IT security certification framework under Title III of this Regulation, propose to the Commission clear minimum requirements for IT security for IT devices sold in or exported from the Union, such as:
	(a) the manufacturer providing a written certification that the device does not contain any hardware, software or firmware component with any known

exploitable security vulnerabilities;

(b) the device relying on software or firmware components capable of accepting properly authenticated and trusted updates from the manufacturer;

(c) the device not including any unencrypted password or access code; the manufacturer documenting the device's remote access capabilities and securing it against unauthorised access during the installation at the latest; the manufacturer not hardcoding default standard passwords in the device; the vendor documenting user possibilities for updating devices and clearly pointing out where responsibilities lie if the user does not update the device;

(d) the obligation for the manufacturer, distributer and importer of internet-connected devices, software, or firmware components of notifying the competent authorities of any known exploitable security vulnerabilities;

(e) the obligation for manufacturers of internet-connected devices, software, or firmware components of providing a repair or replacement in respect of any new security vulnerability discovered;

(f) the obligation for manufacturers of internet-connected devices, software, or firmware components of providing information on how the device is receiving IT security updates, on what the anticipated timeline for ending the IT security support is and on what the user notification process is;

2. The Agency may propose that the minimum IT security requirements referred to in paragraph 1 apply to IT devices from one or more specific sectors.

3. The Agency shall review and, where necessary, amend the IT security requirements referred to in paragraph 1 every two years, and submit any amendments as proposals to the

Commission.

4. The Commission may, by way of implementing acts and based on an impact assessment, decide that the proposed or amended IT security requirements referred to in paragraphs 1 and 2 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

5. The Commission shall ensure appropriate publicity of the IT security requirements which have been decided as having general validity in accordance with paragraph 3.

6. The Agency shall collate all proposed IT security requirements and their amendments in a register and shall make them publicly available by way of appropriate means.

Justification

To replace AM 19 point (c) of the Draft Opinion for the sake of clarity. It is important to achieve a resilient IT environment to protect Cybercrime and protect fundamental rights of IT users. High level IT security objectives for a mandatory IT security base line within the Union should therefore be set in this regulation.

Amendment 64

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

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

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')
References	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Committee responsible Date announced in plenary	ITRE 23.10.2017
Opinion by Date announced in plenary	LIBE 23.10.2017
Rapporteur Date appointed	Jan Philipp Albrecht 20.11.2017
Discussed in committee	25.1.2018 8.3.2018
Date adopted	8.3.2018
Result of final vote	+: 35 –: 2 0: 4
Members present for the final vote	Asim Ademov, Jan Philipp Albrecht, Heinz K. Becker, Caterina Chinnici, Rachida Dati, Cornelia Ernst, Kinga Gál, Sylvie Guillaume, Monika Hohlmeier, Filiz Hyusmenova, Dietmar Köster, Barbara Kudrycka, Monica Macovei, Péter Niedermüller, Ivari Padar, Judith Sargentini, Birgit Sippel, Branislav Škripek, Sergei Stanishev, Traian Ungureanu, Josef Weidenholzer, Cecilia Wikström, Kristina Winberg, Auke Zijlstra
Substitutes present for the final vote	Maria Grapini, Sylvia-Yvonne Kaufmann, Jeroen Lenaers, Andrejs Mamikins, Maite Pagazaurtundúa Ruiz, John Procter, Jaromír Štětina, Josep-Maria Terricabras, Axel Voss, Elissavet Vozemberg-Vrionidi
Substitutes under Rule 200(2) present for the final vote	Andrea Bocskor, Reimer Böge, André Elissen, Ramón Jáuregui Atondo, Julia Reda, Rainer Wieland, Patricija Šulin

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

35	+
ALDE	Filiz Hyusmenova, Maite Pagazaurtundúa Ruiz, Cecilia Wikström
ECR	Monica Macovei, John Procter, Branislav Škripek
GUE/NGL	Cornelia Ernst
PPE	Asim Ademov, Heinz K. Becker, Andrea Bocskor, Rachida Dati, Kinga Gál, Barbara Kudrycka, Jeroen Lenaers, Jaromír Štětina, Patricija Šulin, Traian Ungureanu, Elissavet Vozemberg-Vrionidi, Rainer Wieland
S&D	Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Ramón Jáuregui Atondo, Sylvia-Yvonne Kaufmann, Dietmar Köster, Andrejs Mamikins, Péter Niedermüller, Ivari Padar, Birgit Sippel, Sergei Stanishev, Josef Weidenholzer
VERTS/ALE	Jan Philipp Albrecht, Julia Reda, Judith Sargentini, Josep-Maria Terricabras

2	-
ENF	André Elissen, Auke Zijlstra

4	0
EFDD	Kristina Winberg
PPE	Reimer Böge, Monika Hohlmeier, Axel Voss

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

PROCEDURE – COMMITTEE RESPONSIBLE

Title	Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')			
References	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)			
Date submitted to Parliament	13.9.2017			
Committee responsible Date announced in plenary	ITRE 23.10.2017			
Committees asked for opinions Date announced in plenary	AFET 8.2.2018	BUDG 23.10.2017	IMCO 23.10.2017	LIBE 23.10.2017
Not delivering opinions Date of decision	AFET 4.12.2017			
Associated committees Date announced in plenary	IMCO 18.1.2018			
Rapporteurs Date appointed	Angelika Niebler 27.10.2017			
Discussed in committee	21.3.2018	23.4.2018		
Date adopted	10.7.2018			
Result of final vote	+: –: 0:	56 5 1		
Members present for the final vote	Zigmantas Balčytis, Bendt Bendtsen, Xabier Benito Ziluaga, José Blanco López, David Borrelli, Jonathan Bullock, Cristian-Silviu Buşoi, Jerzy Buzek, Angelo Ciocca, Edward Czesak, Jakop Dalunde, Pilar del Castillo Vera, Christian Ehler, Fredrick Federley, Ashley Fox, Adam Gierek, Theresa Griffin, Rebecca Harms, Barbara Kappel, Krišjānis Kariņš, Jeppe Kofod, Jaromír Kohlíček, Peter Kouroumbashev, Zdzisław Krasnodębski, Christelle Lechevalier, Janusz Lewandowski, Edouard Martin, Tilly Metz, Csaba Molnár, Nadine Morano, Angelika Niebler, Morten Helveg Petersen, Miroslav Poche, Paul Rübig, Massimiliano Salini, Algirdas Saudargas, Sven Schulze, Neoklis Sylikiotis, Dario Tamburrano, Patrizia Toia, Evžen Tošenovský, Vladimir Urutchev, Kathleen Van Brempt, Henna Virkkunen, Lieve Wierinck, Hermann Winkler, Anna Záborská, Flavio Zanonato, Carlos Zorrinho			
Substitutes present for the final vote	Michał Boni, Rosa D'Amato, Eugen Freund, Gunnar Hökmark, Benedek Jávor, Werner Langen, Olle Ludvigsson, Marisa Matias, Gesine Meissner, Pavel Telička			
Substitutes under Rule 200(2) present for the final vote	Romeo Franz, Emilian Pavel, Ulrike Rodust			
Date tabled	30.7.2018			

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

56	+
ALDE	Fredrick Federley, Gesine Meissner, Morten Helveg Petersen, Pavel Telička, Lieve Wierinck
ECR	Edward Czesak, Ashley Fox, Zdzisław Krasnodębski, Evžen Tošenovský
EFDD	Rosa D'Amato, Dario Tamburrano
ENF	Barbara Kappel, Christelle Lechevalier
NI	David Borrelli
PPE	Bendt Bendtsen, Michał Boni, Cristian-Silviu Buşoi, Jerzy Buzek, Pilar del Castillo Vera, Christian Ehler, Gunnar Hökmark, Krišjānis Kariņš, Werner Langen, Janusz Lewandowski, Nadine Morano, Angelika Niebler, Paul Rübig, Massimiliano Salini, Algirdas Saudargas, Sven Schulze, Vladimir Urutchev, Henna Virkkunen, Hermann Winkler, Anna Záborská
S&D	Zigmantas Balčytis, José Blanco López, Eugen Freund, Adam Gierek, Theresa Griffin, Jeppe Kofod, Peter Kouroumbashev, Olle Ludvigsson, Edouard Martin, Csaba Molnár, Emilian Pavel, Miroslav Poche, Ulrike Rodust, Patrizia Toia, Kathleen Van Brempt, Flavio Zanonato, Carlos Zorrinho
VERTS/ALE	Jakop Dalunde, Romeo Franz, Rebecca Harms, Benedek Jávor, Tilly Metz

5	-
EFDD	Jonathan Bullock
GUE/NGL	Xabier Benito Ziluaga, Jaromír Kohlíček, Marisa Matias, Neoklis Sylikiotis

1	0
ENF	Angelo Ciocca

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