European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

2017/0225(COD)

9.2.2018

AMENDMENTS
20 - 125

Draft opinion
Jan Philipp Albrecht
Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

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

AM_Com_LegOpinion

Amendment 20
Cornelia Ernst

Proposal for a regulation
Title

Text proposed by the Commission	*Amendment*
Proposal for a	Proposal for a
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 ***security*** certification (''Cybersecurity Act'')
(Text with EEA relevance)	(Text with EEA relevance)

Or. en

Amendment 21
Michał Boni, Carlos Coelho, Frank Engel

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	(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.	information for organisational and individual users about the cybersecurity features of ICT products and services, undermining trust in digital solutions. ***This ambition is at the heart of the European Commission's reform agenda to achieve a digital single market as ICT networks provide the backbone for digital products and services which have the potential to support all aspects of our lives and drive Europe's economic growth. To ensure that the objectives of 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.***

Or. en

Amendment 22
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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	(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.	***and fragmented*** 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.

Or. en

Amendment 23
Cornelia Ernst

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 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. *(This amendment replaces the term "cybersecurity" by the more appropriate term "IT security". It should apply throughout the text.)*

Or. en

Amendment 24
Jaromír Štětina, Roberta Metsola, Axel Voss

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. ***Moreover, the increasingly frequent conduct of malicious cyber operations by third-country actors, both non-state actors and governments, threatens to disrupt democratic processes and to destabilize democratic societies across Europe.*** In order to mitigate ***these risks*** 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

Or. en

Amendment 25
Maria Grapini

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	(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.

children. In order to mitigate this risk to society, all necessary actions need to be taken to improve ***information security against cyberattacks*** 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.

Or. ro

Amendment 26
Cornelia Ernst

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 ***computer oriented*** 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 ***computer oriented*** threats. *(This amendment replaces the misleading term "cyber threat" by the more appropriate term "computer oriented threat". It should apply throughout the text.)*

Or. en

Amendment 27
Cornelia Ernst

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) ***Computer oriented 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 ***IT security*** 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. *(This amendment replaces the term "cyber attack" by the more appropriate term "computer oriented attack". It should apply throughout the text.)*

Or. en

Amendment 28
Maria Grapini

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. 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.

Or. ro

Amendment 29
Michał Boni, Carlos Coelho, Frank Engel

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	(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across

Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, the trust in the digital single market should be further improved by offering transparent information on the level of security of ICT products and services. This can be facilitated by EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors.

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 co-ordinated EU response and*** 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. ***Alongside EU-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.***

Or. en

Amendment 30
Jaromír Štětina, Axel Voss

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	(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and

preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, the trust in the digital single market should be further improved by offering transparent information on the level of security of ICT products and services. ***This can be facilitated by*** EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors.	preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, the trust in the digital single market should be further improved by offering transparent information on the level of ***privacy and*** security of ICT products and services. EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors ***can contribute to this objective***. ***However, voluntary measures implemented by the private sector, inter alia by IoT operators and service providers, should also be encouraged.***
	Or. en

Amendment 31
Maria Grapini

Proposal for a regulation
Recital 5 a (new)

Text proposed by the Commission	*Amendment*
	(5a) Cybersecurity is an aspect of security as a whole, and competence and expertise in security assessment rests with the Member States. Managing the area of freedom, security and justice is a competence that is shared between the Union and the Member States, but, given the impact of cybersecurity on national security, it is in many respects a matter of

national sovereignty. For this reason, as regards the single European certification framework, the role of Member States and of national certification authorities should not be reduced to an advisory one. Member States should have a significant role in the new cybersecurity certification architecture, also taking account of their expertise.

Or. ro

Amendment 32
Michał Boni, Carlos Coelho, Frank Engel

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	(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 ***fulfils the digital single market strategy and together with other instruments, such as 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 introduced obligations concerning security measures and incident notifications across

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.	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.

Or. en

Amendment 33
Monika Beňová

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 cybersecurity policy, it is necessary to review the mandate of ENISA to define its role in the changed cybersecurity ecosystem and ensure it ***undertakes a leading role which will*** effectively ***improve*** 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.

Or. en

Amendment 34
Monika Beňová

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 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.	(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, that the agency ***concludes*** an agreement between the Agency and the host Member State after obtaining the approval of the Management Board of the Agency. ***This agreement should include provisions that ensure proper and efficient performance of its tasks, upon the due process and full discussion by the Management Board of the agency and other relevant stakeholder within the agency a request for auxiliary support, duties to be upheld by the host state may be ratified into the agreement.***

Or. en

Amendment 35
Monika Beňová

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 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 regards should be given to further enhancement of capacity of the Agency.***

Or. en

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 36
Cornelia Ernst

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 as well as the protection of electronic communications. In order for the agency to appropriately be able to address these challenges, close cooperation and frequent consultation with the bodies established under Regulation (EC) 45/2001, Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EC) No 1211/2009 should form an integral part of the agency's activities.

Or. en

Justification

In order to avoid friction and use synergies, close cooperation with the EDPS, national DPA's, the EDPB as well as BEREC are necessary.

Amendment 37
Monika Beňová

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. 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 ***an objectives which*** the Agency is to accomplish ***should be clearly defined*** while ***giving due consideration to the necessary*** flexibility ***of*** its operations. ***Where possible, highest degree of transparency and dissemination of information should be maintained.***

Or. en

Amendment 38
Michał Boni, Carlos Coelho, Frank Engel

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 cybersecurity threat landscape, it is clear that Member States must be supported by more comprehensive, cross-policy approach to building cyber resilience.

Or. en

Amendment 39
Elissavet Vozemberg-Vrionidi

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) To perform its operational tasks, the Agency should make use of the available expertise of CERT-EU through a structured cooperation, in close physical proximity. The structured cooperation will facilitate the necessary synergies and build-up of ENISA's expertise. Where appropriate, dedicated arrangements between the two organisations should be established to define the practical implementation of such cooperation.	(20) To perform its operational tasks, the Agency should make use of the available expertise of CERT-EU through a structured cooperation, in close physical proximity ***when Large-Scale Cybersecurity Incidents and Crises occur in Europe***. The structured cooperation will facilitate the necessary synergies and build-up of ENISA's expertise. Where appropriate, dedicated arrangements between the two organisations should be established to define the practical implementation of such cooperation.

Or. en

Justification

This should happen in accordance with the operational role of ENISA and in special cases only.

Amendment 40
Maria Grapini

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.

Or. ro

Amendment 41
Michał Boni, Carlos Coelho, Frank Engel

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	(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 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

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.

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***.

Or. en

Amendment 42
Jaromír Štětina, Roberta Metsola

Proposal for a regulation
Recital 28

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

accelerating end-user awareness on security of devices.

basic authentication ***to prevent data and identity theft***. The Agency should play a central role in accelerating end-user awareness on security of devices.

Or. en

Amendment 43
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Proposal for a regulation
Recital 28

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

Or. en

Amendment 44
Jaromír Štětina, Roberta Metsola

Proposal for a regulation
Recital 28 a (new)

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

Or. en

Amendment 45
Elissavet Vozemberg-Vrionidi

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	(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 cybersecurity. It should also liaise with authorities dealing with data protection in order to exchange know-how and best practices and provide advice on

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.

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.

Or. en

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 46
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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	(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 ***European and national*** authorities dealing with data protection in order to exchange know-how and best practices and provide advice on cybersecurity aspects that might have an

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.

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.

Or. en

Amendment 47
Michał Boni, Carlos Coelho, Frank Engel

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 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. ***The agency should work together with stakeholder towards developing a EU-wide approach to responsible vulnerabilities disclosure and should promote best practice in this area.***

Or. en

Amendment 48
Jaromír Štětina, Roberta Metsola

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***, hardware and software producers as well as*** 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 ***ensure that the*** products and services that ***they place on the market*** meet cybersecurity standards. In cooperation with competent authorities, ENISA may disseminate information regarding the level of cybersecurity of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the security, including cybersecurity, of their products and services.

Or. en

Amendment 49
Jaromír Štětina, Roberta Metsola

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	(37) Cybersecurity ***threats are a*** global ***challenge***. Closer international cooperation ***is needed to mitigate these threats, in particular as regards information sharing***

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.	***and the development of common*** security standards, including the definition of common norms of behaviour**.** ***Furthermore***, international collaboration in response to network and information security issues ***should be accelerated and a global approach on these issues promoted***. 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**..**

Or. en

Amendment 50
Michał Boni, Carlos Coelho, Frank Engel

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 will specifically consider implementing measures to***

ensure the pan-EU security standards harmonisation for IoT devices.

Or. en

Amendment 51
Michał Boni, Carlos Coelho, Frank Engel

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

Or. en

Amendment 52
Maria Grapini

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 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***, 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 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.

Or. ro

Amendment 53
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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 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.

Or. en

Amendment 54
Jaromír Štětina, Roberta Metsola, Axel Voss

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	(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.	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***, as is their lifecycle,*** 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 ***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.***

Or. en

Amendment 55
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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.

Or. en

Amendment 56
Maria Grapini

Proposal for a regulation
Recital 56 a (new)

Text proposed by the Commission	*Amendment*
	(56a) This European certification process needs to be analysed to avoid increased costs for producers.

Or. ro

Amendment 57
Michał Boni, Carlos Coelho, Frank Engel

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	(57) Recourse to European cybersecurity 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 EU Member States and the criticality of a product or service, it is recognised that, in the future, potentially mandatory schemes for certain***

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.

ICT products and services may begin to evolve in a phased approach for the 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 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.

Or. en

Amendment 58
Daniel Dalton

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,	(57) Recourse to European cybersecurity certification should remain voluntary, unless otherwise provided in 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

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.	introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme.

Or. en

Justification

The scheme should be on a voluntary basis in collaboration with industry, and should not have the potential to become mandatory at the European level. The NIS Directive notes that the security of network and information systems should be promoted through voluntary industry practice.

Amendment 59
Daniel Dalton

Proposal for a regulation
Recital 62

Text proposed by the Commission	*Amendment*
(62) The Agency's support to cybersecurity certification should also include liaising with the Council Security Committee and the relevant national body, regarding the cryptographic approval of products to be used in classified networks.	***deleted***

Or. en

Justification

National cryptography and their approval procedures should remain a Member State competency as they are vital to national security.

Amendment 60
Monika Hohlmeier

Proposal for a regulation
Recital 62

Text proposed by the Commission	*Amendment*
(62) The Agency's support to cybersecurity certification should also include liaising with the Council Security Committee and the relevant national body, regarding the cryptographic approval of products to be used in classified networks.	(62) The Agency's support to cybersecurity certification should also include liaising with the Council Security Committee and the relevant national body, regarding the cryptographic approval of products to be used in classified networks***, which are not excluded from the scope of this Regulation as laid down in Article 3.3***.

Or. en

Amendment 61
Cornelia Ernst

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 ENISA, the "***European Network and Information Security*** Agency", hereinafter 'the Agency'; and

Or. en

Amendment 62
Cornelia Ernst

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	(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of ***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.	prejudice to specific provisions regarding voluntary or mandatory certification in other Union acts.

Or. en

Justification

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

Amendment 63
Jaromír Štětina, Roberta Metsola

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.

Or. en

Justification

Adding important aspect, especially as regards threat assessment.

Amendment 64
Cornelia Ernst

Proposal for a regulation
Title II

Text proposed by the Commission	*Amendment*
ENISA – the “***EU Cybersecurity*** Agency”	ENISA – the “***European Network and Information Security*** Agency”

Or. en

Amendment 65

Maria Grapini

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 a high level of ***information security, in order to prevent cyberattacks*** within the Union.

Or. ro

Amendment 66
Maria Grapini

Proposal for a regulation
Article 3 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Agency shall carry out tasks conferred upon it by Union acts setting out measures for approximating the laws, regulations and administrative provisions of the Member States which are related to ***cybersecurity***.	2. The Agency shall carry out tasks conferred upon it by Union acts setting out measures for approximating the laws, regulations and administrative provisions of the Member States which are related to ***the security of cyberinformation***.

Or. ro

Amendment 67
Maria Grapini

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

implementing policies related to ***cybersecurity***.	***security of cyberinformation, for the purpose of preventing cyberattacks***.

Or. ro

Amendment 68
Monika Beňová

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 Unions cyber 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.

Or. en

Amendment 69
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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 cybersecurity 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.

Or. en

Amendment 70

Elissavet Vozemberg-Vrionidi

Proposal for a regulation
Article 4 – paragraph 6

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

Or. en

Justification

The Agency is important to develop European and international standards on cybersecurity.

Amendment 71
Jaromír Štětina, Roberta Metsola, Axel Voss

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, including by contributing to ***the development of European and international standards on cybersecurity,*** the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus

strengthen trust in the digital internal market.

Or. en

Amendment 72
Cornelia Ernst

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 cybersecurity.

Or. en

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 73
Michał Boni, Carlos Coelho, Frank Engel

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 cybersecurity notably in relation to Directive (EU) 2016/1148***, Directive establishing the European Electronic Communications Code, Regulation (EU) 2016/679 and Directive2002/58/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;

Or. en

Amendment 74
Cornelia Ernst

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

Text proposed by the Commission	*Amendment*
	2 a. assisting the bodies established under Regulation (EU) 2016/679 in developing guidelines setting out conditions and safeguards for further processing of personal data for security purposes with the objective of protecting against attacks against network and information systems within the scope of Regulation (EU) 2016/679, Directive (EU) 2016/1148 and Directive 2002/58/EC;

Or. en

Amendment 75
Cornelia Ernst

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

Text proposed by the Commission	*Amendment*
	2 b. proposing policies setting out conditions and deadlines for the fixing of IT security vulnerabilities by ICT vendors with the objective of avoiding any exposure of users to computer oriented threats;

Or. en

Amendment 76
Cornelia Ernst

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

Text proposed by the Commission	*Amendment*
	2 c. proposing policies for public authorities for handling of vulnerabilities that are not known to the public, with the objective of safeguarding the integrity of the ecosystem of information systems;

Or. en

Amendment 77
Cornelia Ernst

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

Text proposed by the Commission	*Amendment*
	2 d. proposing policies and advising public authorities to avoid and limit the deployment of closed-source IT solutions in order to ensure that the ICT ecosystem is free from vulnerabilities, in particular backdoors;

Or. en

Amendment 78
Elissavet Vozemberg-Vrionidi

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

Text proposed by the Commission	*Amendment*
(a) Member States in their efforts to improve the prevention, detection and	(a) Member States in their efforts to improve the prevention, detection and

analysis, and the capacity to respond to, ***cybersecurity problems*** and incidents by providing them with the necessary knowledge and expertise;	analysis, and the capacity to respond to, ***cyber threats*** and incidents by providing them with the necessary knowledge and expertise;

Or. en

Justification

Better wording.

Amendment 79
Elissavet Vozemberg-Vrionidi

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

Text proposed by the Commission	*Amendment*
(b) Union institutions, bodies, offices and agencies, in their efforts to improve the prevention, detection and analysis of and the capability to respond to ***cybersecurity problems*** and incidents through appropriate support for the CERT for the Union institutions, agencies and bodies (CERT-EU);	(b) Union institutions, bodies, offices and agencies, in their efforts to improve the prevention, detection and analysis of and the capability to respond to ***cyber threats*** and incidents through appropriate support for the CERT for the Union institutions, agencies and bodies (CERT-EU);

Or. en

Justification

Better wording.

Amendment 80
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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

Or. en

Amendment 81
Maria Grapini

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.

Or. ro

Amendment 82
Elissavet Vozemberg-Vrionidi

Proposal for a regulation
Article 7 – paragraph 5 – subparagraph 2

Text proposed by the Commission	*Amendment*
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	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.	investigation concerning the same incident***.*** ***Such enquiry shall not interfere with the essential interests of the Member States to safeguard their national security***. 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.

Or. en

Justification

In addition, the enquiry shall not interfere with the essential interests of the Member States to safeguard their national security.

Amendment 83
Elissavet Vozemberg-Vrionidi

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

Or. en

Justification

In this field the cooperation with industry is important.

Amendment 84
Jaromír Štětina, Roberta Metsola, Axel Voss

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

Or. en

Justification

Linked to the amended article 44.

Amendment 85
Cornelia Ernst

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

Text proposed by the Commission	*Amendment*
	(ba) facilitate the establishment and take-up of European and international standards for the security of ICT products and services, with the objective of preventing the use and distribution, both intentionally and non-intentionally, of technology, or parts thereof, intentionally weakening the security of ICT products and services ('backdoors');

Or. en

Justification

A proper certification scheme should outright ban the use of backdoors in ICT products and services.

Amendment 86
Jaromír Štětina, Roberta Metsola

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, provided by the Union institutions, agencies and bodies ***and made available by Member States and public and private stakeholders***;

Or. en

Amendment 87
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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***, disseminate adequate measures for prevention of incidents***, and provide guidance on good practices for individual users aimed at citizens and organisations;

Or. en

Amendment 88
Jaromír Štětina, Roberta Metsola

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 cybersecurity education and awareness.

Or. en

Justification

The creation of this network under Agency´s umbrella should allow national responsible bodies to be more aware of activities developed in other Member States, it should intensify spreading best practises in e.g. developing cyber security specialisation curricula.

Amendment 89
Jaromír Štětina, Roberta Metsola

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 cybersecurity and its visibility in the Union.

Or. en

Amendment 90
Elissavet Vozemberg-Vrionidi

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***,*** Union institutions, bodies, offices***,*** agencies regular ***and industry*** outreach campaigns to increase cybersecurity and its visibility in the Union.

Or. en

Justification

In this field the cooperation with industry is important.

Amendment 91
Elissavet Vozemberg-Vrionidi

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

Text proposed by the Commission	*Amendment*
	(ga) Support closer coordination and exchange of best practices among Member States on cybersecurity education and awareness by facilitating creation and maintenance of a network of national education points of contact;

Or. en

Justification

The coordination and best practices exchange among Member States through a network of national education points of contact raise awareness on cybersecurity issues.

Amendment 92
Cornelia Ernst

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 cybersecurity ***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;

Or. en

Amendment 93
Daniel Dalton

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 area of cybersecurity ***only***, 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;

Or. en

Justification

ENISA has a clear remit regarding cybersecurity, and work on other related matters such as data protection and privacy are covered by existing executive agencies and should not be duplicated.

Amendment 94
Maria Grapini

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;

Or. ro

Amendment 95
Elissavet Vozemberg-Vrionidi

Proposal for a regulation
Article 19 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Executive Director shall decide whether it is necessary to locate members of staff in one or more Member States for the purpose of carrying out the Agency's tasks in an efficient and effective manner. Before deciding to establish a local office the Executive Director shall obtain the prior consent of the Commission, the Management Board and the Member State(s) concerned. The decision shall specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and duplication of administrative functions of the Agency. An agreement with the Member State(s) concerned shall be reached, where appropriate or required.	***deleted***

Or. en

Justification

The field of responsibilities of ENISA does not require presence in other Member States as for example FRONTEX and EASO that are special cases. Moreover, this practice will create additional costs and an increased budget.

Amendment 96
Michał Boni, Carlos Coelho, Frank Engel

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	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.	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 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.

Or. en

Amendment 97
Daniel Dalton

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

Text proposed by the Commission	*Amendment*
	5a. The Permanent Stakeholders' Group shall be consulted on the preparation of candidate schemes referred to in Article 44(1) as part of an official consultation process, alongside wider industry stakeholders.

Or. en

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 98
Jaromír Štětina

Proposal for a regulation
Article 30 – paragraph 1

Text proposed by the Commission	*Amendment*

1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[39] , the Agency shall***, within six months from the day it becomes operational,*** accede to the Interinstitutional Agreement of 25 May, 1999 concerning internal investigations by the European Anti-fraud Office (OLAF) and shall adopt the appropriate provisions applicable to all the employees of the Agency, using the template set out in the Annex to that Agreement.	1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[39] , the Agency shall accede to the Interinstitutional Agreement of 25 May, 1999 concerning internal investigations by the European Anti-fraud Office (OLAF) and shall adopt ***without delay*** the appropriate provisions applicable to all the employees of the Agency, using the template set out in the Annex to that Agreement.
[39] Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).	[39] Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

Or. en

Amendment 99
Jaromír Štětina, Roberta Metsola

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.

Or. en

Amendment 100
Michał Boni, Carlos Coelho, Frank Engel

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') ***or the Permanent Stakeholders' Group*** established under Article ***20 and 53 respectively*** may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.

Or. en

Amendment 101
Jaromír Štětina, Axel Voss

Proposal for a regulation
Article 44 – paragraph 1

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

Or. en

Justification

Ensuring consistency with recital 53. Explicit collaboration with private sector stakeholders re-enforces the inclusiveness of the process.

Amendment 102
Michał Boni, Carlos Coelho, Frank Engel

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 all relevant 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.***

Or. en

Amendment 103
Cornelia Ernst

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 ***as well as with the bodies established under Regulation (EC) 45/2001, Regulation (EU) 2016/679, Directive (EU) 2016/680 and, if appropriate, Regulation (EC) No 1211/2009*** . 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.

Or. en

Amendment 104
Daniel Dalton

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 all relevant stakeholders***, including industry through an official consultation process,*** 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.

Or. en

Justification

Industry as well as standardisation organisations 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 105

Monika Hohlmeier

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 ***after approval by the Group*** to the Commission.

Or. en

Amendment 106
Cornelia Ernst

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 cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation. ***Where appropriate, the Commission shall consult the European Data Protection Board before adopting such decision in order to ensure consistency with certifications under Regulation (EU) 2016/679.***

Or. en

Amendment 107
Daniel Dalton

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 ***in proportion to risks to their common operational environment, and where users take appropriate measures***, the following security objectives:

Or. en

Justification

Security objectives should offer flexibility to account for the use of ICT devices and services in different situations and users' necessary role in achieving some security objectives

Amendment 108
Daniel Dalton

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 assurance levels: basic, substantial and/or high, for ICT products and services issued under that scheme***, including for their different individual use cases***.

Or. en

Justification

Offers flexibility for vendors to apply different assurance levels to different use cases of ICT products and services.

Amendment 109
Michał Boni, Carlos Coelho, Frank Engel

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 cybersecurity certification scheme, which provides a corresponding 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; the assurance level shall be defined on a case by case basis.***

Or. en

Amendment 110
Michał Boni, Carlos Coelho, Frank Engel

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***

Or. en

Amendment 111
Daniel Dalton

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

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

Or. en

Justification

We should not risk consumers becoming over reliant on certificates, nor push industry to spend time and resource in obtaining a high level of assurance, thereby delaying time to market and reducing responsiveness to demand, without addressing preventative user action.

Amendment 112
Michał Boni, Carlos Coelho, Frank Engel

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,	***deleted***

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

Or. en

Amendment 113
Daniel Dalton

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 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***, given appropriate measures are taken by users***;

Or. en

Justification

As above.

Amendment 114
Michał Boni, Carlos Coelho, Frank Engel

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	***deleted***

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.

Or. en

Amendment 115
Daniel Dalton

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

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

Or. en

Justification

As above.

Amendment 116
Michał Boni, Carlos Coelho, Frank Engel

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

Or. en

Amendment 117
Michał Boni, Carlos Coelho, Frank Engel

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 cybersecurity certification schemes***, pursuant to Article 49,*** covering the same type or categories of ICT products and services;

Or. en

Amendment 118
Daniel Dalton

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. The certification shall be voluntary.

Or. en

Justification

The scheme should be on a voluntary basis in collaboration with industry, and should not have the potential to become mandatory at the European level. The NIS Directive notes that

the security of network and information systems should be promoted through voluntary industry practice.

Amendment 119
Daniel Dalton

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 of ***time as defined by the certification scheme*** and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.

Or. en

Justification

Certifications can take 12 to 18 months to achieve, and reflect security at a point in time for a specific product.

Amendment 120
Monika Hohlmeier

Proposal for a regulation
Article 48 – paragraph 6

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

Or. en

Amendment 121

Michał Boni, Carlos Coelho, Jaromír Štětina, Frank Engel

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*** and may be renewed provided that the relevant requirements continue to be met.

Or. en

Amendment 122
Jan Philipp Albrecht

Proposal for a regulation
Article 48 a (new)

Text proposed by the Commission	*Amendment*
	Article 48a
	Baseline IT security requirements
	1. The agency shall, by ... [two years after the date of entry into force of this regulation], propose to the Commission clear and mandatory baseline IT security requirements for all IT devices sold in or exported from the Union such as:
	(a) the vendor providing a written certification that the device does not contain any hardware, software or firmware component with any known security vulnerabilities;
	(b) the device relies on software or firmware components capable of accepting properly authenticated and trusted updates from the vendor;
	(c) documented remote access capabilities of the device that are secured against unauthorized access during the installation at the latest; no default

hardcoded standard passwords for all devices, a documented possibility for updates which clearly points out responsibilities in case the user does not update the device;

(d) an obligation of the vendor of the internet-connected device, software, or firmware component to notify the competent authority of any known security vulnerabilities;

(e) an obligation of the vendor of the internet-connected device, software, or firmware component to provide a repair or replacement in respect to any new security vulnerability discovered;

(f) an obligation of the vendor of the internet-connected device, software, or firmware component to provide information on how the device receives updates, the anticipated timeline for ending security support and a formal notification when such security support has ended.

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

3. The Commission may, by way of implementing acts, decide that the proposed or amended 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 set out in Article 55(2).

4. The Commission shall ensure appropriate publicity for the requirements which have been decided as having general validity in accordance with paragraph 3.

5. The Agency shall collate all proposed requirements and their amendments in a register and shall make

them publicly available by way of appropriate means.

Or. en

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 123
Cornelia Ernst

Proposal for a regulation
Article 48 a (new)

Text proposed by the Commission	*Amendment*
	Article 48 a
	Minimum requirements for IT security
	1. The Agency shall, by ... [two years after the date of entry into force of this Regulation], propose to the Commission clear and mandatory minimum requirements of security for all IT devices sold in or exported from the Union such as:
	(a) the vendor providing a legally binding written certification that the device does not contain any hardware, software or firmware component with any known security vulnerabilities;
	(b) the device relies on software or firmware components capable of accepting properly authenticated and trusted updates from the vendor;
	(c) the device does not include any fixed or hard-coded credential used for remote administration, the delivery of updates, or communication;
	(d) an obligation of the vendor of the internet-enabled device, software, or

firmware component to notify the competent authority of any known security vulnerabilities;

(e) an obligation of the vendor of the internet-enabled device, software, or firmware component to provide a repair or replacement in respect to any new security vulnerability discovered;

(f) an obligation of the vendor of the internet-enabled device, software, or firmware component to provide information on how the device receives updates, the anticipated timeline for ending security support and a formal notification when such security support has ended.

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

3. The Commission shall, by way of implementing acts, decide that the proposed or amended 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 set out in Article 55(2).

4. The Commission shall ensure appropriate publicity for the requirements which have been decided as having general validity in accordance with paragraph 3.

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

Or. en

Justification

This is a slightly improved version of the rapporteurs' proposal.

Amendment 124
Daniel Dalton

Proposal for a regulation
Article 48 a (new)

Text proposed by the Commission	*Amendment*
	Article 48 a
	Baseline IT security requirements
	1. The Agency shall, by ... [two years after the date of entry into force of this Regulation], propose to the Commission clear baseline IT security requirements for all IT devices sold in or exported from the Union, which industry should be encouraged to generally adhere to where appropriate, such as:
	(a) the vendor providing a written certification that the device does not contain any hardware, software or firmware component with any known security vulnerabilities;
	(b) the device relies on software or firmware components capable of accepting properly authenticated and trusted updates from the vendor;
	(c) the device does not include any unencrypted password or access code. However, the use of secure elements used for remote administration, the delivery of updates, or communication, is strongly encouraged;
	(d) an obligation of the vendor of the internet-connected device, software, or firmware component to notify the competent authority of any known security vulnerabilities;
	(e) an obligation of the vendor of the internet-connected device, software, or firmware component to provide a repair or replacement in respect to any new security vulnerability discovered;

	(f) an obligation of the vendor of the internet-connected device, software, or firmware component to provide information on how the device receives updates, the anticipated timeline for ending security support and a formal notification when such security support has ended.
	2. The Agency shall review and, where necessary, amend the requirements referred to in paragraph 1 every two years, and submit any amendments as proposals to the Commission.

Or. en

Justification

Amends the Rapporteur's proposal to make baseline IT security requirements voluntary and applicable where appropriate. As regards (C), the rapporteur's proposal had been formulated in a way that may lead to misunderstandings. Whereas unencrypted credentials may lead to weaker protection, the use of hard-coded data in objects such as secure elements provides additional security.

Amendment 125
Cornelia Ernst

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 cybersecurity certification schemes;

Or. en

Justification

From the EDPS opinion.