European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

2017/0225(COD)

16.3.2018

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on Industry, Research and Energy

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

Rapporteur: Jan Philipp Albrecht

PA_Legam

SHORT JUSTIFICATION

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

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

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

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

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

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

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

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

and IT security measures;

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

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

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

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

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

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

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

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

AMENDMENTS

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

Amendment 1

Proposal for a regulation
Title

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

Justification

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

Amendment 2

Proposal for a regulation
Recital 2

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

use of certification leads to insufficient information for ***organisational*** and individual users about the ***cybersecurity*** features of ICT products and services, undermining trust in digital solutions.

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

Amendment 3

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) Cyber-attacks are on the increase and a connected economy and society that 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	(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 ***IT security*** authorities and law enforcement competences are predominantly national. Large-scale cyber incidents could disrupt the provision of essential services across the EU. This requires effective EU level response and crisis management, building upon dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of ***IT security*** and resilience in the Union, based on reliable Union data, as well as systematic forecast of future developments, challenges and threats, both at Union and global level, is therefore important for policy makers,

users	industry and users.

Amendment 4

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) In light of the increased ***cybersecurity*** challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on ***cybersecurity*** issues. Moreover, the trust in the digital single market should be further improved by offering transparent information on the level of security of ICT products and services. This can be facilitated by EU-wide certification providing common ***cybersecurity*** requirements and evaluation criteria across national markets and sectors.	(5) In light of the increased ***IT security*** challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to ***deliver a coordinated EU response and*** increase awareness of citizens and businesses on ***IT security*** issues. Moreover, the trust in the digital single market should be further improved by offering transparent information on the level of security of ICT products and services. This can be facilitated by EU-wide certification providing common ***IT security*** requirements and evaluation criteria across national markets and sectors. ***Alongside Union-wide certification, there is a range of voluntary measures widely accepted in the market place, depending on the product, service, use or standard. These measures as well as the industry bottom up approach, including the use of security-by-design, leveraging and contributing to international standards, should be encouraged.***

Amendment 5

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) The Union has already taken important steps to ensure ***cybersecurity*** and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to ***cybersecurity*** threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of ***cybersecurity***, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). The NIS Directive ***put*** in place requirements concerning national capabilities in the area of ***cybersecurity***, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for economy and society such as energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces). A key role was attributed to ENISA in supporting implementation of this Directive. In addition, effective fight against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of ***cybersecurity***.	(7) The Union has already taken important steps to ensure ***IT security*** and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to ***IT security*** threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of ***IT security***, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). The NIS Directive ***fulfils the digital single market strategy and together with other instruments, such as Directive .../... [establishing the European Electronic Communications Code], Regulation (EU) 2016/679 of the European Parliament and of the Council[1a] and Directive 2002/58/EC of the European Parliament and of the Council[1b], puts*** in place requirements concerning national capabilities in the area of ***IT security***, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for economy and society such as energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces). A key role was attributed to ENISA in supporting implementation of this Directive. In addition, effective fight against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of ***IT***

security.

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

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

Amendment 6

Proposal for a regulation
Recital 8

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

Amendment 7

Proposal for a regulation
Recital 11

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

Justification

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

Amendment 8

Proposal for a regulation
Recital 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) The challenges in the field of IT security are, in the digital age, often closely interlinked with challenges in the field of data protection, the protection of private life and the protection of electronic communications. In order for the agency to be able to address those challenges appropriately, there is a need for close cooperation and frequent consultation with the bodies established under Regulation (EC) 45/2001of the European Parliament and of the Council[1a], Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EC) No 1211/2009 as well as with

industry and civil society.

[1a] Regulation (EC) 45/2001of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Amendment 9

Proposal for a regulation
Recital 12

Text proposed by the Commission	*Amendment*
(12) The Agency should develop and maintain a high level of expertise and operate as a point of reference establishing trust and confidence in the single market by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in carrying out its tasks. The Agency should proactively contribute to 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 ***and objectives which*** the Agency is to accomplish ***should be clearly defined*** while ***giving due consideration to the necessary*** flexibility ***of*** its operations. ***Where possible, the highest degree of transparency and dissemination of information should be maintained.***

Amendment 10

Proposal for a regulation
Recital 14

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

Amendment 11

Proposal for a regulation
Recital 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) The Commission should propose the introduction of mandatory cooperation between Member States concerning the protection of critical information infrastructure.

Amendment 12

Proposal for a regulation
Recital 26

Text proposed by the Commission	*Amendment*
(26) To understand better the challenges in the field of ***cybersecurity***, and with a view to providing strategic long term advice to Member States and Union institutions, the Agency needs to analyse current and emerging risks. For that	(26) To understand better the challenges in the field of ***IT security***, and with a view to providing strategic long term advice to Member States and Union institutions, the Agency needs to analyse current and emerging risks***, incidents and***

purpose, the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information and perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on network and information security, in particular ***cybersecurity***. The Agency should furthermore support Member States and Union institutions, agencies and bodies in identifying emerging trends and preventing problems related to ***cybersecurity***, by performing analyses of threats ***and*** incidents.

vulnerabilities. For that purpose, the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information and perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on network and information security, in particular ***IT security***. The Agency should furthermore support Member States and Union institutions, agencies and bodies in identifying emerging trends and preventing problems related to ***IT security***, by performing analyses of threats***,*** incidents ***and vulnerabilities***.

Amendment 13

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) The Agency should contribute towards raising the awareness of the public about risks related to ***cybersecurity*** and provide guidance on good practices for 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	(28) The Agency should contribute towards raising the awareness of the public about risks related to ***IT security*** and provide guidance on good practices for individual users aimed at citizens and organisations. ***To improve the overall level of preparedness and resilience,*** the Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing available information regarding significant incidents and by compiling reports with a view to providing guidance to businesses***,*** citizens and ***relevant authorities at Union and national*** level. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users***. These campaigns should promote IT security education and*** safer individual online behaviour and ***raise***

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.	awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, ***forgery and illegal content,*** as well as ***advocating data protection and*** basic authentication ***to prevent data and identity theft***. The Agency should play a central role in accelerating end-user awareness on security of devices.

Amendment 14

Proposal for a regulation
Recital 28 a (new)

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

Amendment 15

Proposal for a regulation
Recital 30

Text proposed by the Commission	*Amendment*
(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational management of large-scale IT systems (eu-LISA), European Aviation Safety Agency (EASA) and any other EU Agency that is involved in ***cybersecurity***. It should also liaise with authorities dealing with data protection in order to exchange know-how and best practices and provide advice on	(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational management of large-scale IT systems (eu-LISA), European Aviation Safety Agency (EASA***), European Global Navigation Satellite Systems Agency (GSA***) and any other EU Agency that is involved in ***IT security***. It should also liaise with ***Union and national*** authorities dealing with data

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.

protection in order to exchange know-how and best practices and provide advice on ***IT security*** aspects that might have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the Agency's Permanent Stakeholders Group. In liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks.

Justification

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

Amendment 16

Proposal for a regulation
Recital 35

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

approach to the responsible disclosure of vulnerabilities and should promote best practice in this area.

Amendment 17

Proposal for a regulation
Recital 44

Text proposed by the Commission	*Amendment*
(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the attention of the Agency. The composition of the Permanent Stakeholders Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure sufficient representation of stakeholders in the work of the Agency.	(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the attention of the Agency. The composition of the Permanent Stakeholders Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure sufficient representation of stakeholders in the work of the Agency. ***Given the importance of certification requirements to ensure trust in IoT, the Commission should specifically consider implementing measures to ensure Union-wide harmonisation of security standards for IoT devices.***

Amendment 18

Proposal for a regulation
Recital 50

Text proposed by the Commission	*Amendment*
(50) Currently, the ***cybersecurity*** certification of ICT products and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry	(50) Currently, the ***IT security*** certification of ICT products and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry

driven schemes. In this context, a certificate issued by one national ***IT security*** authority is not in principle recognised by other Member States. Companies thus may have to certify their products and services in several Member States where they operate, for example with a view to participating in national procurement procedures. 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.

driven schemes. In this context, a certificate issued by one national ***IT security*** authority is not in principle recognised by other Member States. Companies thus may have to certify their products and services in several Member States where they operate, for example with a view to participating in national procurement procedures***, and these procedures may entail additional costs for companies***. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach with regard to horizontal ***IT security*** issues, for instance in the field of the Internet of Things. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual utilisation. ***A case-by-case approach should ensure that services and products are subject to appropriate certification schemes. Additionally, a risk-based approach is needed for effective identification and mitigation of risks and to avoid increased costs for manufacturers.***

Amendment 19

Proposal for a regulation
Recital 52

Text proposed by the Commission	*Amendment*
(52) In view of the above, it is necessary to establish a European ***cybersecurity*** certification framework laying down the main horizontal requirements for European ***cybersecurity*** certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it should avoid the	(52) In view of the above, it is necessary to establish a ***harmonised*** European ***IT security*** certification framework laying down the main horizontal requirements for European ***IT security*** certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it

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.

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

Amendment 20

Proposal for a regulation
Recital 55

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

then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications.	then be further specified in detail at the level of the individual certification scheme adopted by the Commission ***in close consultation with the Member States and industrial stakeholders***, for example by reference to standards or technical specifications. ***The individual certification schemes should be designed in such a way that all actors involved in the development of relevant IT products and services are encouraged to develop and adopt standards, norms and principles which ensure the highest possible level of security throughout the lifecycle.***

Amendment 21

Proposal for a regulation
Recital 55 a (new)

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

Amendment 22

Proposal for a regulation
Recital 56

Text proposed by the Commission	*Amendment*
(56) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services. The Commission, based on the candidate scheme proposed by ENISA, should then be empowered to adopt the European ***cybersecurity*** certification scheme by means of implementing acts. Taking account of the	(56) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services. The Commission, based on the candidate scheme proposed by ENISA, should then be empowered to adopt the European ***IT security*** certification scheme by means of implementing acts. Taking account of the

general purpose and security objectives identified in this Regulation, European ***cybersecurity*** certification schemes adopted by the Commission should specify a minimum set of elements concerning the subject-matter, the scope and functioning of the individual scheme. These should include among others the scope and object of the ***cybersecurity*** certification, including the categories of ICT products and services covered, the detailed specification of the ***cybersecurity*** requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods, as well as the intended level of assurance: basic, substantial and/or high.

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

Amendment 23

Proposal for a regulation
Recital 57

Text proposed by the Commission	*Amendment*
(57) Recourse to European ***cybersecurity*** certification should remain voluntary, unless otherwise provided in Union or national legislation. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national ***cybersecurity*** certification schemes or procedures for the ICT products and services covered by a European ***cybersecurity*** certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act. Moreover, Member States should not introduce new national certification	(57) Recourse to European ***IT security*** certification should remain voluntary, unless otherwise provided in Union or national legislation. ***After this initial stage, and depending on the maturity of implementation in the Member States and the criticality of a product or service, potentially mandatory certification schemes for certain ICT products and services may be introduced in a phased approach for future generations of technology and in response to the policy objectives of tomorrow.*** However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national ***IT security***

schemes providing ***cybersecurity*** certification schemes for ICT products and services already covered by an existing European ***cybersecurity*** certification scheme.	certification schemes or procedures for the ICT products and services covered by a European ***IT security*** certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act. Moreover, Member States should not introduce new national certification schemes providing ***IT security*** certification schemes for ICT products and services already covered by an existing European ***IT security*** certification scheme.

Amendment 24

Proposal for a regulation
Recital 58 a (new)

Text proposed by the Commission	*Amendment*
	(58a) Clear baseline IT security requirements should be devised by the Agency, and should be proposed to the Commission as implementing acts if appropriate, for all IT devices sold in or exported from the Union. Those requirements should be revised every two years thereafter, in order to ensure ongoing improvements. Those baseline IT security requirements should require, inter alia, that devices not contain any known exploitable security vulnerability, that they be capable of accepting trusted security updates, that the vendor notify the competent authorities of known vulnerabilities and repair or replace affected devices up until the time a manufacturer has made clear that security support for such devices will end.

Amendment 25

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

Text proposed by the Commission	*Amendment*

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

Justification

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

Amendment 26

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

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

Justification

Adding important aspect, especially as regards threat assessment.

Amendment 27

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

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

Amendment 28

Proposal for a regulation
Article 4 – paragraph 5

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

Amendment 29

Proposal for a regulation
Article 4 – paragraph 6

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

Amendment 30

Proposal for a regulation
Article 4 – paragraph 7

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

Justification

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

Amendment 31

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

Text proposed by the Commission	*Amendment*
2. assisting Member States to implement consistently the Union policy and law regarding ***cybersecurity*** notably in relation to Directive (EU) 2016/1148, including by means of opinions, guidelines, advice and best practices on topics such as risk management, incident reporting and information sharing, as well as facilitating the exchange of best practices between competent authorities in this regard;	2. assisting Member States to implement consistently the Union policy and law regarding ***IT security*** notably in relation to Directive (EU) 2016/1148***, Directive .../... [establishing the European Electronic Communications Code], Regulation (EU) 2016/679 and Directive 2002/58/EC***, including by means of opinions, guidelines, advice and best practices on topics such as risk management, incident reporting and information sharing, as well as facilitating the exchange of best practices between competent authorities in this regard;

Amendment 32

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

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

their information systems in the context of:

(i) Regulation (EU) 2016/679;

(ii) Directive (EU) 2016/1148; and

(iii) Directive 2002/58/EC;

Amendment 33

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

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

Amendment 34

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

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

Amendment 35

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

Text proposed by the Commission	*Amendment*
	2d. proposing guidelines, in

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

Amendment 36

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

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

Amendment 37

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

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

Amendment 38

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

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

Amendment 39

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

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

Amendment 40

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

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

Justification

ENISA should advise legislators regarding the preparation of policies to allow the EU to catch up with IT security industries in third countries. The project should be comparable in

scale to what has previously been achieved in the aviation industry (example of Airbus). This is needed to develop a stronger, sovereign and trustworthy EU ICT industry (see the Scientific Foresight Unit (STOA) study PE 614.531).

Amendment 41

Proposal for a regulation
Article 7 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Upon a request by ***two or more*** Member ***States concerned***, and with the sole purpose of providing advice for the prevention of future incidents, the Agency shall provide support to or carry out an ex-post technical enquiry following notifications by affected undertakings of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148. The Agency shall also carry out such an enquiry upon a duly justified request from the Commission in agreement with the concerned Member States in case of such incidents affecting more than two Member States.	5. Upon a request by ***a*** Member ***State***, and with the sole purpose of providing advice for the prevention of future incidents, the Agency shall provide support to or carry out an ex-post technical enquiry following notifications by affected undertakings of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148. The Agency shall also carry out such an enquiry upon a duly justified request from the Commission in agreement with the concerned Member States in case of such incidents affecting more than two Member States.
The scope of the enquiry and the procedure to be followed in conducting such enquiry shall be agreed by the concerned Member 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.	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 ***or to Member States' national security measures***. The enquiry shall be concluded by a final technical report compiled by the Agency in particular on the basis of information and comments provided by the concerned Member States and undertaking(s) and agreed with the concerned Member States. A summary of the report focussing on the recommendations for the prevention of future incidents will be shared with the CSIRTs network.

Amendment 42

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

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

Justification

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

Amendment 43

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

Text proposed by the Commission	*Amendment*
(1) preparing candidate European ***cybersecurity*** certification schemes for ICT products and services in accordance with Article 44 of this Regulation;	(1) preparing candidate European ***IT security*** certification schemes for ICT products and services in ***cooperation with industry and in*** accordance with Article 44 of this Regulation;

Justification

In this field the cooperation with industry is important.

Amendment 44

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

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

Justification

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

Amendment 45

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

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

Amendment 46

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

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

Amendment 47

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

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

Amendment 48

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

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

Amendment 49

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

Text proposed by the Commission	*Amendment*
	(ga) promote the widespread adoption by all actors on the EU Digital Single Market of preventive strong IT security measures and reliable privacy enhancing technologies as the first line of defence against attacks against information systems.

Justification

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

Amendment 50

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

Text proposed by the Commission	*Amendment*
(a) advise the Union and the Member States on research needs and priorities in the ***area*** of ***cybersecurity***, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;	(a) advise the Union and the Member States on research needs and priorities in the ***areas*** of ***IT security and data protection and privacy***, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;

Amendment 51

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

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

Amendment 52

Proposal for a regulation
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services	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.

available to the public, consumer groups, ***the European standardisation organisations,*** academic experts in the ***IT security***, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities.

Amendment 53

Proposal for a regulation
Article 30 – paragraph 2

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

Amendment 54

Proposal for a regulation
Article 44 – paragraph 2

Text proposed by the Commission	*Amendment*
2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant 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.

Justification

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

Amendment 55

Proposal for a regulation
Article 44 – paragraph 4

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

Justification

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

Amendment 56

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

Text proposed by the Commission	*Amendment*
2. The assurance levels basic, substantial and high shall ***meet the following criteria respectively:***	2. The assurance levels basic, substantial and high shall ***refer to a certificate issued in the context of a European IT security certification***

	scheme, which provides a corresponding degree of confidence in the claimed or asserted IT security qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related to those standards, including technical controls, the purpose of which is to decrease the risk of IT security incidents.

Amendment 57

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

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

Amendment 58

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

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

of which is to decrease substantially the risk of cybersecurity incidents;

Amendment 59

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

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

Amendment 60

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

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

Amendment 61

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

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

Amendment 62

Proposal for a regulation
Article 48 – paragraph 6

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

Amendment 63

Proposal for a regulation
Article 48 a (new)

Text proposed by the Commission	*Amendment*
	Article 48a
	Baseline IT security requirements
	1. The Agency shall, based on its experience with the IT security certification framework under Title III of this Regulation, propose to the Commission clear minimum requirements for IT security for IT devices sold in or exported from the Union, such as:
	(a) the manufacturer providing a written certification that the device does not contain any hardware, software or firmware component with any known exploitable security vulnerabilities;
	(b) the device relying on software or firmware components capable of accepting properly authenticated and trusted updates from the manufacturer;
	(c) the device not including any unencrypted password or access code; the manufacturer documenting the device's remote access capabilities and securing it against unauthorised access during the installation at the latest; the manufacturer not hardcoding default standard

passwords in the device; the vendor documenting user possibilities for updating devices and clearly pointing out where responsibilities lie if the user does not update the device;

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

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

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

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

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

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

5. The Commission shall ensure appropriate publicity of the IT security

	requirements which have been decided as having general validity in accordance with paragraph 3.
	6. The Agency shall collate all proposed IT security requirements and their amendments in a register and shall make them publicly available by way of appropriate means.

Justification

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

Amendment 64

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

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

Justification

From the EDPS opinion.

PROCEDURE – COMMITTEE ASKED FOR OPINION

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

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

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

2	-
ENF	André Elissen, Auke Zijlstra

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

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