European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

2017/0225(COD)

17.1.2018

DRAFT 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*
Proposal for a 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 on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology ***IT security*** certification ("Cybersecurity Act") *(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)*

Or. en

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 58 a (new)

Text proposed by the Commission	*Amendment*
	(58a) Clear and mandatory 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 developed within two years after the date of entry into force of this Regulation and revised every two years thereafter, in order to ensure constant and dynamic improvements. Those baseline IT security requirements should require, inter alia, that the device does not contain any known security

	vulnerability that it is capable of accepting trusted security updates, that the vendor notifies competent authorities of known vulnerabilities and repairs or replaces the affected device, or that the vendor informs when security support for such device will end.

Or. en

Justification

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 3

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 Agenc***y"***, hereinafte***r **'**the Agency'; and	(a) lays down the objectives, tasks and organisational aspects of ENISA, the ***EU Network and Information Security Agency(***the **"**Agency"***)***; and

Or. en

Justification

The Rapporteur proposes keeping the original name of ENISA (the EU Network and Information Security Agency).

Amendment 4

Proposal for a regulation
Title II

Text proposed by the Commission	*Amendment*
ENISA – the "EU ***Cybersecurity*** Agency"	ENISA – the ***EU Network and Information***

Security Agency

Or. en

Justification

The Rapporteur proposes keeping the original name of ENISA (the EU Network and Information Security Agency).

Amendment 5

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

Text proposed by the Commission	*Amendment*
	2a. assisting the European Data Protection Board established by Regulation (EU) 2016/679 in developing guidelines: to specify at the technical level the conditions allowing the licit use of personal data by data controllers for IT security purposes with the objective of protecting their infrastructure by detecting and blocking attacks against their information systems in the context of:
	(i) Regulation (EU) 2016/679[1a];
	(ii) Directive (EU) 2016/1148[1b]; and
	(iii) Directive 2002/58/EC[1c];
	[1a] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).
	[1b] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network

and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[1c] 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).

Or. en

Amendment 6

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

Text proposed by the Commission	*Amendment*
	2b. proposing policies with the objective of ensuring that ICT vendors act with due diligence regarding the timely fixing of IT security vulnerabilities in their products and services in order to avoid unduly exposing their users to cybercrime;

Or. en

Justification

Establishing a correct break down of responsibilities is essential to encourage all stakeholders to act with due diligence.

Amendment 7

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

Text proposed by the Commission	*Amendment*
	2c. proposing policies establishing a

strong responsibility and liability framework for all stakeholders (including end-users) taking part in ICT eco-systems;

Or. en

Amendment 8

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

Text proposed by the Commission	*Amendment*
	2d. proposing policies strengthening regulation 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 of 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;

Or. en

Justification

Operators of critical infrastructures should be responsible for obtaining some assurance that only secure and trustworthy users/participants use their infrastructure and if needed should isolate un-secure ones to avoid incidents.

Amendment 9

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

Text proposed by the Commission	*Amendment*
	2e. proposing policies 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;

Or. en

Justification

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.

Amendment 10

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

Text proposed by the Commission	*Amendment*
	2f. proposing policies 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;

Or. en

Justification

Adequate EU policies are needed to implement a coherent responsible disclosure processes across the EU.

Amendment 11

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

Text proposed by the Commission	*Amendment*
	2g. proposing policies 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 absence of backdoors and other possible security vulnerabilities;

Or. en

Justification

The use of open-source software should be encouraged in public administrations that should also accept the related responsibilities of checking the source code of the applications that they use (against the presence/absence of major IT security vulnerabilities).

Amendment 12

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.

Or. en

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 13

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 States, regular independent IT security audits of critical infrastructures with the objective of identifying possible recommendations to strengthen their resilience.

Or. en

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 14

Proposal for a regulation
Article 8 – 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.

Or. en

Justification

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

Amendment 15

Proposal for a regulation
Article 9 – 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.

Or. en

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 16

Proposal for a regulation
Article 10 – 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

Justification

Based on the EDPS opinion. Research tasks of ENISA in the field of data protection and

privacy were in the previous Regulation 526/2013 but are no longer in the Commission proposal. The disappearance of this task in research and advice is likely to lead to the discontinuation of ENISA's work on privacy and data protection enhancing technologies (PET) and more in general on data protection by design and by default.

Amendment 17

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 ***as well as with the Article 29 Working Party and the European Data Protection Board***. 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

Based on the EDPS opinion. It is of the utmost importance that technical and governance synergies be created so that certifications under the European Cybersecurity Certification Framework and under the GDPR are not perceived as contradictory or unrelated by the organisations striving for compliance with the relevant instruments.

Amendment 18

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	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.	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. ***The Commission may consult the European Data Protection Board and take account of its view before adopting such implementing acts.***

Or. en

Justification

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

Amendment 19

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) 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-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

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.