European Parliament
2019-2024

Committee on Industry, Research and Energy

2022/0272(COD)

31.3.2023

***I
DRAFT REPORT

on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Committee on Industry, Research and Energy

Rapporteur: Nicola Danti

Symbols for procedures

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

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

Amendments to a draft act

Amendments by Parliament set out in two columns

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

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

Amendments by Parliament in the form of a consolidated text

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

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2022)0454),

– having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0308/2022),

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

– having regard to the opinion of the European Economic and Social Committee of 14 December 2022[1],

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

– having regard to the opinions of the Committee on Civil Liberties, Justice and Home Affairs and the Committee on the Internal Market and Consumer Protection,

– having regard to the report of the Committee on Industry, Research and Energy (A9-0000/2023),

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

2. Requests the Commission to modify the financial statement accompanying the proposal by increasing the establishment plan of the European Union Agency for Cybersecurity (ENISA) by 8,5 additional full-time postsand by providing corresponding additional appropriations in order to ensure that the obligations of ENISA under this Regulation can be fulfilled and not to compromise existing obligations of the Agency under other Union legislation;

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

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

[1] OJ C 100, 16.3.2023, p. 101.

Amendment 1

Proposal for a regulation
Recital 1

Text proposed by the Commission	*Amendment*
(1) It is necessary to improve the functioning of the internal market by laying down a uniform ***legal*** framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.	(1) ***Cybersecurity is one of the key challenges for the Union and the number and variety of connected devices will rise exponentially in the coming years. Cyberattacks are also on the rise and have a critical impact not just on the Union's economy, but also on democracy and society in the Union.*** It is ***therefore*** necessary to ***strengthen the Union's approach to cybersecurity and cyber resilience and to*** improve the functioning of the internal market by laying down a uniform ***regulatory*** framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

Or. en

Amendment 2

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) This Regulation aims to set the boundary conditions for the development of secure products with digital elements by	(2) This Regulation aims to set the boundary conditions for the development of secure products with digital elements by

ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements***, for example by improving transparency with regard to the expected lifetime of products placed on the market and the provision of security updates***.

Or. en

Amendment 3

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) While the existing Union legislation applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on ***companies*** to comply with a number of requirements for similar types of products. The cybersecurity of these products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level. The Union regulatory landscape should be harmonised by introducing cybersecurity requirements	(4) While the existing Union legislation applies to certain products with digital elements, there is no horizontal Union regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on ***undertakings*** to comply with a number of requirements for similar types of products. The cybersecurity of these products has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level***, to ensure a harmonised and clear regulatory framework for undertakings, particularly***

for products with digital elements. In addition, certainty for operators and users should be ensured across the Union, as well as a better harmonisation of the single market, creating more viable conditions for operators aiming at entering the Union market.	***micro, small and medium-sized enterprises***. The Union regulatory landscape should be harmonised by introducing cybersecurity requirements for products with digital elements. In addition, certainty for operators and users should be ensured across the Union, as well as a better harmonisation of the single market, creating more viable conditions for operators aiming at entering the Union market.

Or. en

Amendment 4

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) The horizontal nature of this Regulation means that it will have an impact on very different segments of the Union's economy. It is therefore important that the specificities of each sector are taken into account and that the cybersecurity requirements laid down in this Regulation are proportional to the risks, in order to avoid overburdening specific sectors. The Commission should issue and publish guidelines, including with regard to those matters, to assist businesses in implementing this Regulation.

Or. en

Amendment 5

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) At Union level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade[16] , the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021,[17] have called for specific Union cybersecurity requirements for digital or connected products, with several countries around the world introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe,[18] citizens called for "a stronger role for the EU in countering cybersecurity threats".	(5) At Union level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade[16] , the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021[17] have called for specific Union cybersecurity requirements for digital or connected products, with several countries around the world introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe,[18] citizens called for "a stronger role for the EU in countering cybersecurity threats". ***In order for the Union to play a leading international role in the field of cybersecurity, it is important to establish an ambitious overarching regulatory framework.***
[16] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.	[16] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.
[17] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html.	[17] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html.
[18] Conference on the Future of Europe – Report on the Final Outcome, May 2022, Proposal 28(2). The Conference was held Between April 2021 and May 2022. It was a unique, citizen-led exercise of deliberative democracy at the pan-European level, involving thousands of European citizens as well as political actors, social partners, civil society representatives and key stakeholders.	[18] Conference on the Future of Europe – Report on the Final Outcome, May 2022, Proposal 28(2). The Conference was held Between April 2021 and May 2022. It was a unique, citizen-led exercise of deliberative democracy at the pan-European level, involving thousands of European citizens as well as political actors, social partners, civil society representatives and key stakeholders.

Or. en

Amendment 6

Proposal for a regulation
Recital 8

Text proposed by the Commission	*Amendment*
(8) By setting cybersecurity requirements for placing on the market products with digital elements, the cybersecurity of these products for consumers and for businesses alike will be enhanced. This also includes requirements for placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitors.	(8) By setting cybersecurity requirements for placing on the market products with digital elements, the cybersecurity of these products for consumers and for businesses alike will be enhanced. This also includes requirements for placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitors. ***Those requirements will also ensure that cybersecurity is taken into account throughout supply chains, for the purpose of making final products with digital elements more secure. This will, in turn, represent a competitive advantage for manufacturers established or represented in the Union, which will be able to showcase the cybersecurity of their products.***

Or. en

Amendment 7

Proposal for a regulation
Recital 9

Text proposed by the Commission	*Amendment*
(9) This Regulation ensures a high level of cybersecurity of products with digital elements. It does not regulate services, such as Software-as-a-Service (SaaS), except for remote data processing solutions relating to a product with digital elements understood as any data processing at a distance for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that	(9) This Regulation ensures a high level of cybersecurity of products with digital elements. It does not regulate services, such as Software-as-a-Service (SaaS), except for remote data processing solutions relating to a product with digital elements understood as any data processing at a distance for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that

manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions. ***[Directive XXX/XXXX (NIS2)]*** puts in place cybersecurity and incident reporting requirements for essential and important entities, such as critical infrastructure, with a view to increasing the resilience of the services they provide. ***[Directive XXX/XXXX (NIS2)]*** applies to cloud computing services and cloud service models, such as SaaS. All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope of that Directive.

manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its ***core*** functions. ***Directive (EU) 2022/2555*** puts in place cybersecurity and incident reporting requirements for essential and important entities, such as critical infrastructure, with a view to increasing the resilience of the services they provide. ***Directive (EU) 2022/2555*** applies to cloud computing services and cloud service models, such as SaaS. All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope of that Directive.

Or. en

Amendment 8

Proposal for a regulation
Recital 10

Text proposed by the Commission	*Amendment*
(10) In order not to hamper innovation or research, free and open-source software ***developed or*** supplied ***outside*** the course of a commercial activity should ***not*** be covered by this Regulation***. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable***. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.	(10) In order not to hamper innovation or research, ***only*** free and open-source software supplied ***in*** the course of a commercial activity should be covered by this Regulation. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. ***Where free and open-source software has been developed or supplied outside the course of a commercial activity, manufacturers that incorporate such software in their products with digital elements should take all the necessary steps to ensure the***

compliance with this Regulation.

Or. en

Amendment 9

Proposal for a regulation
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) Products with digital elements that are developed exclusively for national security or military purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation. However, Member States are encouraged to ensure the same or higher level of protection for those products as for those falling within the scope of this Regulation.

Or. en

Amendment 10

Proposal for a regulation
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) This Regulation should not apply to components that are exclusively manufactured in order to replace identical components during repair operations in legacy products with digital elements, in order to avoid products with digital elements already circulating in the internal market having to be withdrawn due to the lack of spare parts.

Or. en

Amendment 11

Proposal for a regulation
Recital 14 b (new)

Text proposed by the Commission	*Amendment*
	(14b) Leasing companies are not considered to be distributors for the purposes of this Regulation, insofar as their activities qualify solely as finance or credit provisions in support of the activities of the manufacturers or other economic operators.

Or. en

Justification

Leasing companies acting as third-party for financing purposes in leasing contracts should not qualify as distributors, provided that their activities are only focused on the financing element.

Amendment 12

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(15) Delegated Regulation (EU) 2022/30 specifies that the essential requirements set out in Article 3(3), point (d) (network harm and misuse of network resources), point (e) (personal data and privacy) and point (f) (fraud) of Directive 2014/53/EU apply to certain radio equipment. [Commission implementation decision XXX/2022 on a standardisation request to the European Standardisation Organisations] lays down requirements for the development of specific standards further specifying how these three essential requirements should be addressed. The essential requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e)	(15) Delegated Regulation (EU) 2022/30 specifies that the essential requirements set out in Article 3(3), point (d) (network harm and misuse of network resources), point (e) (personal data and privacy) and point (f) (fraud) of Directive 2014/53/EU apply to certain radio equipment. [Commission implementation decision XXX/2022 on a standardisation request to the European Standardisation Organisations] lays down requirements for the development of specific standards further specifying how these three essential requirements should be addressed. The essential requirements laid down by this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e)

and (f) of Directive 2014/53/EU. Further, the essential requirements laid down in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, if the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation.	and (f) of Directive 2014/53/EU. Further, the essential requirements laid down in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, if the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation. ***Where manufacturers comply with this Regulation before its date of application, they shall be considered also to comply with Delegated Regulation (EU) 2022/30, until the Commission repeals that Delegated Regulation.***
	Or. en

Amendment 13

Proposal for a regulation
Recital 18 a (new)

Text proposed by the Commission	*Amendment*
	(18a) When procuring products with digital elements, Member States should give priority to products that have a high level of cybersecurity and an appropriate expected product lifetime, in order to improve their ability to deal with cyber threats, as well as to ensure the efficient use of public resources. Furthermore, Member States should ensure that manufacturers remedy vulnerabilities that affect publicly procured products with

digital elements as a matter of urgency.

Or. en

Amendment 14

Proposal for a regulation
Recital 19

Text proposed by the Commission	*Amendment*
(19) Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of ***Directive [Directive XXX / XXXX (NIS2)]***, and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in ***Directive [Directive XXX / XXXX (NIS2)]***. Furthermore, considering its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or	(19) Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as ***significant*** incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of ***Directive (EU) 2022/2555***, and inform the relevant market surveillance authorities about the notified vulnerability***. ENISA should ensure that such notifications are received, stored and transmitted via secure channels and that clear protocols are in place with regard to who can access them and the arrangements for their onward transmission. ENISA should not release to the public information about vulnerabilities for which a security update is not available***. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in ***Directive (EU) 2022/2555***. Furthermore, considering its expertise and mandate, ENISA should be able to support

identify categories of products for which simultaneous coordinated control actions should be organised. In exceptional circumstances, at the request of the Commission, ENISA should be able to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.

the process for implementation of this Regulation. In particular, it should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which simultaneous coordinated control actions should be organised. In exceptional circumstances, at the request of the Commission, ENISA should be able to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the good functioning of the internal market.

Or. en

Amendment 15

Proposal for a regulation
Recital 19 a (new)

Text proposed by the Commission	*Amendment*
	(19a) ENISA should publish notified vulnerabilities in the European vulnerability database established under Directive (EU) 2022/2555. ENISA should have in place an appropriate procedure regarding the publication process in order to give manufacturers the time to develop the necessary security updates and users the time to implement them or take other corrective or mitigating measures. The database is intended to help manufacturers detect known exploitable vulnerabilities and understand their criticality, in order to place on the market more secure products.

Or. en

Amendment 16

Proposal for a regulation
Recital 27

Text proposed by the Commission	*Amendment*
(27) The categories of critical products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation lists products which are defined by their core functionality as general purpose microprocessors in class II. As a result, general purpose microprocessors are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a general purpose microprocessor. The Commission should adopt delegated acts [by ***12*** months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III.	(27) The categories of critical products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation lists products which are defined by their core functionality as general purpose microprocessors in class II. As a result, general purpose microprocessors are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a general purpose microprocessor. The Commission should adopt delegated acts [by ***6*** months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III. ***In order to ensure legal clarity and certainty, amendments to the list in Annex III should be made no more frequently than once every two years and should be adopted only after a thorough evaluation by the Commission, including consultation of stakeholders.***

Or. en

Amendment 17

Proposal for a regulation
Recital 27 a (new)

Text proposed by the Commission	*Amendment*
	(27a) The Commission should set up an expert group on cyber resilience (the 'Expert Group'), with a wide and diverse membership. The Expert Group should support the Commission in order to ensure the proper implementation of this Regulation, for example by advising the Commission on possible amendments to the list of critical products as set out in Annex III or by analysing in what way European and international standards can enable compliance with the essential requirements of this Regulation.

Or. en

Amendment 18

Proposal for a regulation
Recital 32

Text proposed by the Commission	*Amendment*
(32) In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as throughout their life-cycle, it is necessary to lay down essential requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential requirements related to vulnerability handling ***and ensure that all their products are delivered without any known exploitable vulnerabilities***, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product. For this purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital	(32) In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as throughout their life-cycle, it is necessary to lay down essential requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential requirements related to vulnerability handling ***throughout the expected product lifetime***, they should determine which other essential requirements related to the product properties are relevant for the concerned type of product. For this purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential requirements and in order

elements to identify relevant risks and relevant essential requirements and in order to appropriately apply suitable harmonised standards or common specifications.

to ***deliver their products without known exploitable vulnerabilities that might have an impact on the security of those products and to*** appropriately apply suitable harmonised standards or common specifications.

Or. en

Amendment 19

Proposal for a regulation
Recital 32 a (new)

Text proposed by the Commission	*Amendment*
	(32a) Manufacturers should ensure, where possible and in particular in the case of business-to-consumer products, that security updates are installed automatically in order to remedy potential vulnerabilities as soon as possible. Users should retain the possibility to de-activate this feature. Once a product with digital elements has reached the end of its expected product lifetime and security updates are no longer made available, manufacturers should inform users in a simple and clear manner, for example via the display of a user-friendly notification.

Or. en

Amendment 20

Proposal for a regulation
Recital 32 b (new)

Text proposed by the Commission	*Amendment*
	(32b) Where manufacturers set the expected period lifetime to a period shorter than five years and therefore no longer offer security updates for the product with digital elements, they should

make their source code available to undertakings that wish to provide security updates and other similar services. Such access should be made available only as part of a contractual arrangement that protects the ownership of the product with digital elements and prevents the dissemination of the source code to the general public. The obligation to provide free access to the source code should be in place only for five years after the product with digital elements has been placed on the market.

Or. en

Amendment 21

Proposal for a regulation
Recital 34

Text proposed by the Commission	*Amendment*
(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of ***Directive [Directive XX/XXXX (NIS2)]*** are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should ***also consider disclosing*** fixed vulnerabilities to the European vulnerability database established under ***Directive [Directive XX/XXXX (NIS2)]*** and managed by ENISA ***or under any other publicly accessible vulnerability***	(34) To ensure that the national CSIRTs and the single point of contacts designated in accordance with Article [Article X] of ***Directive (EU) 2022/2555*** are provided with the information necessary to fulfil their tasks and raise the overall level of cybersecurity of essential and important entities, and to ensure the effective functioning of market surveillance authorities, manufacturers of products with digital elements should notify to ENISA vulnerabilities that are being actively exploited. ***Mandatory notification should not apply to vulnerabilities that are discovered by ethical security hackers operating with no malicious intent and with the manufacturer's consent.*** As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered a threat to the functioning of the internal market. Manufacturers should ***disclose*** fixed vulnerabilities to the European

database.	vulnerability database established under ***Directive (EU) 2022/2555*** and managed by ENISA.

Or. en

Justification

Vulnerabilities discovered by white hats should not be subject to mandatory reporting.

Amendment 22

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) Manufacturers should also report to ENISA any incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in ***Directive [Directive XXX/XXXX (NIS2)]*** for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in accordance with Article [Article X] of ***Directive [Directive XXX/XXXX (NIS2)]*** and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.	(35) Manufacturers should also report to ENISA any ***significant*** incident having an impact on the security of the product with digital elements. Notwithstanding the incident reporting obligations in ***Directive (EU) 2022/2555*** for essential and important entities, it is crucial for ENISA, the single points of contact designated by the Member States in accordance with Article [Article X] of ***Directive (EU) 2022/2555*** and the market surveillance authorities to receive information from the manufacturers of products with digital elements allowing them to assess the security of these products. In order to ensure that users can react quickly to ***significant*** incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the risks, by reaching out to the users directly.

Or. en

Amendment 23

Proposal for a regulation
Recital 35 a (new)

Text proposed by the Commission	*Amendment*
	(35a) Manufacturers, other, entities and actors should also be able to report to ENISA, on a voluntary basis, about other cybersecurity incidents, cyber threats, near misses and any other vulnerability.

Or. en

Justification

In line with the introduction of an article enabling voluntary additional reporting.

Amendment 24

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties.	(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties. ***Manufacturer should not, however, be obliged to make the software bill of materials public, as***

this may have unintended consequences on the cybersecurity of their products with digital elements.

Or. en

Amendment 25

Proposal for a regulation
Recital 41

Text proposed by the Commission	*Amendment*
(41) Where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. ***Reasons for developing such common specifications, instead of relying on harmonised standards, might include a refusal of*** the standardisation ***request by any of the European standardisation organisations,*** undue delays in the establishment of appropriate harmonised standards***, or a lack of compliance of developed standards*** with the ***requirements of this Regulation or with a*** request ***of the Commission***. In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.	(41) Where no harmonised standards are adopted or where the harmonised standards do not sufficiently address the essential requirements of this Regulation, the Commission should be able to adopt common specifications by means of implementing acts. ***Such option should be seen as an exceptional 'fall back' solution, when*** the standardisation ***process is blocked, where there are*** undue delays in the establishment of appropriate harmonised standards ***or where the deliverables fail to comply*** with the ***initial*** request. In order to facilitate assessment of conformity with the essential requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements.

Or. en

Justification

In line with the changes to Article 19 and the GPSR, making common specification as a last-resort option

Amendment 26

Proposal for a regulation
Recital 45

Text proposed by the Commission	*Amendment*
(45) As a general rule the conformity assessment of products with digital elements should be carried out by the manufacturer under its own responsibility following the procedure based on Module A of Decision 768/2008/EC. The manufacturer should retain flexibility to choose a stricter conformity assessment procedure involving a third-party. If the product is classified as a critical product of class I, additional assurance is required to demonstrate conformity with the essential requirements set out in this Regulation. The manufacturer should apply harmonised standards, common specifications or cybersecurity certification schemes under Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act, if it wants to carry out the conformity assessment under its own responsibility (module A). If the manufacturer does not apply such harmonised standards, common specifications or cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party. Taking into account the administrative burden on manufacturers and the fact that cybersecurity plays an important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures respectively based on modules B+C or module H of Decision 768/2008/EC have been chosen as most appropriate for assessing the compliance of critical products with digital elements in a proportionate and effective manner. The manufacturer that carries out the third-	(45) As a general rule the conformity assessment of products with digital elements should be carried out by the manufacturer under its own responsibility following the procedure based on Module A of Decision 768/2008/EC. The manufacturer should retain flexibility to choose a stricter conformity assessment procedure involving a third-party. If the product is classified as a critical product of class I, additional assurance is required to demonstrate conformity with the essential requirements set out in this Regulation. The manufacturer should apply harmonised standards, common specifications or cybersecurity certification schemes under Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act, if it wants to carry out the conformity assessment under its own responsibility (module A)***, provided that that those harmonised standards, common specifications or cybersecurity certification schemes have been in place for a minimum period of time enabling manufacturers to adopt them***. If the manufacturer does not apply such harmonised standards, common specifications or cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party. Taking into account the administrative burden on manufacturers and the fact that cybersecurity plays an important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures respectively based on modules B+C or module H of Decision 768/2008/EC have

party conformity assessment can choose the procedure that suits best its design and production process. Given the even greater cybersecurity risk linked with the use of products classified as critical class II products, the conformity assessment should always involve a third party.

been chosen as most appropriate for assessing the compliance of critical products with digital elements in a proportionate and effective manner. The manufacturer that carries out the third-party conformity assessment can choose the procedure that suits best its design and production process. Given the even greater cybersecurity risk linked with the use of products classified as critical class II products, the conformity assessment should always involve a third party.

Or. en

Amendment 27

Proposal for a regulation
Recital 46 a (new)

Text proposed by the Commission	*Amendment*
	(46a) This Regulation places complex obligations on economic operators, particularly for manufacturers of software products and for micro, small and medium-sized enterprises. The Commission should therefore issue guidelines in the form of a handbook for economic operators, which explains in a detailed and clear manner the practical implications of this Regulation. Those guidelines should cover inter alia an explanation of the notion of remote data processing, a description of the methodology used to determine critical products with digital elements and an illustration of the interaction between this Regulation and other Union law.

Or. en

Amendment 28

Proposal for a regulation
Recital 53

Text proposed by the Commission	*Amendment*
(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden ***for*** economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.	(53) In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden ***on*** economic operators***. The Commission and Member States should therefore ensure that there is a sufficient availability of skilled professionals in the Union, so that notified conformity assessment bodies can carry out their activities quickly and efficiently and that bottlenecks are minimised***. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.

Or. en

Amendment 29

Proposal for a regulation
Recital 61

Text proposed by the Commission	*Amendment*
(61) Simultaneous coordinated control actions (‘sweeps’) are specific enforcement actions by market surveillance authorities that can further enhance product security. Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps could be organised to the	(61) Simultaneous coordinated control actions (‘sweeps’) are specific enforcement actions by market surveillance authorities that can further enhance product security. Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks. ENISA should submit proposals for categories of products for which sweeps could be organised to the

market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives.	market surveillance authorities, based, among others, on the notifications of product vulnerabilities and incidents it receives. ***Specific attention should be given to products with digital elements placed on the market by manufacturers that might present a security risk for the Union, including in light of the geopolitical context.***

Or. en

Amendment 30

Proposal for a regulation
Recital 61 a (new)

Text proposed by the Commission	*Amendment*
	(61a) Concerns about economic operators that might present a security risk for the Union should, however, require that appropriate safeguards are put in place and thorough scrutiny of their products with digital elements is ensured. Thus, ENISA should perform a coordinating role to ensure that market surveillance authorities carry out regular checks of such products with digital elements, in particular to identify potential embedded backdoors or other exploitable vulnerabilities.

Or. en

Amendment 31

Proposal for a regulation
Recital 62

Text proposed by the Commission	*Amendment*
(62) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in	(62) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in

accordance with Article 290 of the Treaty should be delegated to the Commission in respect of updates to the list of critical products in Annex III and specifying the definitions of the these product categories. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential mandating of certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[33] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

accordance with Article 290 of the Treaty should be delegated to the Commission in respect of updates to the list of critical products in Annex III and specifying the definitions of the these product categories. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential mandating of certification of certain highly critical products with digital elements based on criticality crieria set out in this Regulation, as well as for specifying the minimum content of the EU declaration of conformity and supplementing the elements to be included in the technical documentation. ***The Commission should also specify the format and elements of the software bill of materials, specify further the type of information, format and procedure of the notifications on actively exploited vulnerabilities and significant incidents submitted to ENISA by the manufacturers. Where necessary, the Commission should be empowered to adopt delegated acts to adopt common specifications in respect of the essential requirements set out in Annex I.*** It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level***, and particularly with the Expert Group***, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making[33] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all

documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

[33] OJ L 123, 12.5.2016, p. 1.

[33] OJ L 123, 12.5.2016, p. 1.

Or. en

Justification

Alignment with new delegated acts, including where the Commission proposal foresees implementing acts.

Amendment 32

Proposal for a regulation
Recital 63

Text proposed by the Commission	*Amendment*
(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to: ***specify the format and elements of the software bill of materials, specify further the type of information, format and procedure of the notifications on actively exploited vulnerabilities and incidents submitted to ENISA by the manufacturers,*** specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts therefore as set out in Annex I of this Regulation***, adopt common specifications in respect of the essential requirements set out in Annex I***, lay down technical specifications for pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use, decide on corrective or restrictive measures at Union level in exceptional circumstances	(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to: specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts therefore as set out in Annex I of this Regulation, lay down technical specifications for pictograms or any other marks related to the security of the products with digital elements, and mechanisms to promote their use, decide on corrective or restrictive measures at Union level in exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[34] .

which justify an immediate intervention to preserve the good functioning of the internal market. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[34] .

[34] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

[34] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

Or. en

Justification

Delegated acts are more appropriate for these elements.

Amendment 33

Proposal for a regulation
Recital 65

Text proposed by the Commission	*Amendment*
(65) In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. Maximum levels for administrative fines to be provided for in national laws for non-compliance with the obligations laid down in this Regulation should therefore be established. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation should be taken into account and as a minimum those explicitly established in this Regulation, including whether administrative fines have been already	(65) In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. Maximum levels for administrative fines to be provided for in national laws for non-compliance with the obligations laid down in this Regulation should therefore be established. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation should be taken into account and as a minimum those explicitly established in this Regulation, including whether administrative fines have been already

applied by other market surveillance authorities to the same operator for similar infringements. Such circumstances can be either aggravating, in situations where the infringement by the same operator persists on the territory of other Member States than the one where an administrative fine has already been applied, or mitigating, in ensuring that any other administrative fine considered by another market surveillance authority for the same economic operator or the same type of breach should already take account, along with other relevant specific circumstances, of a penalty and the quantum thereof imposed in other Member States. In all such cases, the cumulative administrative fine that could be applied by market surveillance authorities of several Member States to the same economic operator for the same type of infringement should ensure the respect of the principle of proportionality.	applied by other market surveillance authorities to the same operator for similar infringements***, as well as whether the economic operator is a micro, small or medium sized enterprise***. Such circumstances can be either aggravating, in situations where the infringement by the same operator persists on the territory of other Member States than the one where an administrative fine has already been applied, or mitigating, in ensuring that any other administrative fine considered by another market surveillance authority for the same economic operator or the same type of breach should already take account, along with other relevant specific circumstances, of a penalty and the quantum thereof imposed in other Member States. In all such cases, the cumulative administrative fine that could be applied by market surveillance authorities of several Member States to the same economic operator for the same type of infringement should ensure the respect of the principle of proportionality.

Or. en

Amendment 34

Proposal for a regulation
Recital 66 a (new)

Text proposed by the Commission	*Amendment*
	(66a) The revenue generated from imposing penalties pursuant to this Regulation should be used to raise the level of cybersecurity within the Union, promoting programmes aiming to support the enhancement and best use of European knowledge, capacity and skills related to cybersecurity and the sharing and mainstreaming of best practices. To that end, that revenue should be allocated to the Cybersecurity and Trust Specific Objective of the Digital Europe

	Programme referred to in Article 6 of Regulation (EU) 2021/694. Those funds should be considered to be a top-up of that budget line and should not reduce the contribution from the Union's budget.

Or. en

Amendment 35

Proposal for a regulation
Recital 68

Text proposed by the Commission	*Amendment*
(68) The Commission should periodically review this Regulation, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.	(68) The Commission should periodically review this Regulation, in consultation with ***the Expert Group and other*** interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

Or. en

Amendment 36

Proposal for a regulation
Recital 69

Text proposed by the Commission	*Amendment*
(69) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. This Regulation should apply [***24*** months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [***12*** months] from the entry into force of this Regulation.	(69) Economic operators should be provided with a sufficient time to adapt to the requirements of this Regulation. This Regulation should apply [***40*** months] from its entry into force, with the exception of the reporting obligations concerning actively exploited vulnerabilities and incidents, which should apply [***20*** months] from the entry into force of this Regulation.

Or. en

Justification

Sufficient time should be provided to economic operators to adapt to this Regulation, in light of its horizontal nature, broad scope and complexity.

Amendment 37

Proposal for a regulation
Recital 69 a (new)

Text proposed by the Commission	*Amendment*
	(69a) In order to support micro, small and medium-sized enterprises and to help them respond to the additional costs that may result from this Regulation, the Commission should put in place adequate financial and technical support enabling those undertakings to contribute to the growth of the European economy and to increase the level of its cybersecurity.

Or. en

Amendment 38

Proposal for a regulation
Recital 71 a (new)

Text proposed by the Commission	*Amendment*
	(71a) The Commission should amend the legislative financial statement accompanying this Regulation by providing ENISA with 8,5 additional full-time posts and corresponding additional appropriations in order to fulfil its additional tasks provided for in this Regulation.

Or. en

Amendment 39

Proposal for a regulation
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Regulation applies to products with digital elements ***whose intended or reasonably foreseeable use includes*** a direct or indirect ***logical or physical*** data connection to a device or network.	1. This Regulation applies to products with digital elements ***that can have*** a direct or indirect data connection to a device or network.

Or. en

Justification

It is necessary to simplify the scope, in order to make it more understandable for citizens and businesses alike.

Amendment 40

Proposal for a regulation
Article 2 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. This Regulation does not apply to components that are exclusively manufactured as spare parts for other products with digital elements that have been placed on the market before ... [40 months after the date of entry into force of this Regulation].

Or. en

Justification

In order ensure that products already on the market prior to the entry into force of this Regulation can be repaired and their lifetime extended, it is necessary to provide for an exemption for spare parts.

Amendment 41

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

Text proposed by the Commission	*Amendment*
(2) 'remote data processing' means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;	(2) 'remote data processing' means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its ***core*** functions;

Or. en

Justification

Remote data processing solutions should be covered when they are pivotal to the functioning of the product with digital elements.

Amendment 42

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

Text proposed by the Commission	*Amendment*
	(4a) 'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

Or. en

Justification

Reference to the definition of cybersecurity contained in the Cyber Security Act.

Amendment 43

Proposal for a regulation
Article 3 – paragraph 1 – point 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) 'micro, small and medium sized enterprises' means micro, small and medium sized enterprises as defined in Commission Recommendation 2003/361/EC[1a];
	[1a] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

Or. en

Amendment 44

Proposal for a regulation
Article 3 – paragraph 1 – point 39 a (new)

Text proposed by the Commission	*Amendment*
	(39a) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

Or. en

Amendment 45

Proposal for a regulation
Article 3 – paragraph 1 – point 39 b (new)

Text proposed by the Commission	*Amendment*
	(39b) 'near miss' means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;

Or. en

Justification

The definition of near miss, contained in NIS 2, will be used for voluntary reporting in the newly created Article 11a.

Amendment 46

Proposal for a regulation
Article 3 – paragraph 1 – point 39 c (new)

Text proposed by the Commission	*Amendment*
	(39c) 'cyber threat' means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

Or. en

Justification

The definition of cyber threat, contained in the Cyber Security Act, will be used for voluntary reporting in the newly created Article 11a.

Amendment 47

Proposal for a regulation
Article 6 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list of categories of critical products with digital elements a new category or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into account:	2. ***After ... [two years after the date of entry into force of this Regulation] and no more frequently than every two years thereafter,*** the Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list of categories of critical products with digital elements a new category or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements. In determining the level of cybersecurity risk, one or several of the following criteria shall be taken into

account:

Or. en

Justification

For the sake of legal clarity and predictability, it is necessary to ensure that the list of critical products can be amended only once every two years.

Amendment 48

Proposal for a regulation
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by ***12*** months since the entry into force of this Regulation].	3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by ***6*** months since the entry into force of this Regulation].

Or. en

Justification

A rapid definition of the product categories is essential to give undertakings enough time to adapt to this Regulation.

Amendment 49

Proposal for a regulation
Article 6 – paragraph 4 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Where a new category of critical products with digital elements is added to the list in Annex III by means of a delegated act pursuant to paragraph 2 of this Article, it shall be subject to the relevant conformity assessment procedures referred to in Article 24(2) and (3) within 12 months of

the date of adoption of the related delegated act.

Or. en

Justification

Manufacturers of critical products that are already listed in Annex III will benefit from a transitional period between entry into force and implementation of this Regulation. Hence, a transitional period should also be envisaged for critical products that are newly added to the list after the entry into force of this Regulation.

Amendment 50

Proposal for a regulation
Article 6 – paragraph 5 – introductory part

Text proposed by the Commission	*Amendment*
5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. ***The obligation to obtain a European cybersecurity certificate shall apply 12 months after the adoption of the relevant delegated act.*** When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is:

Or. en

Justification

A transitional period of 12 months should apply for products which will be required to obtain a European cybersecurity certificate.

Amendment 51

Proposal for a regulation
Article 6 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. The Commission is empowered to adopt the delegated acts referred to in paragraph 5 of this Article no earlier than 12 months after the adoption of the relevant European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881.

Or. en

Justification

A minimum period of operation for new European cybersecurity certification schemes should be envisaged, to ensure their correct operation and give sufficient time to undertakings to adopt them.

Amendment 52

Proposal for a regulation
Article 6 – paragraph 5 b (new)

Text proposed by the Commission	*Amendment*
	5b. Before adopting the delegated acts referred to in paragraphs 2, 4 and 5 of this Article, the Commission shall consult the Expert Group referred to in [Article 6a].

Or. en

Justification

Stakeholder consultation will be essential to the functioning of this Regulation. The

Commission should consult extensively the newly created Expert Group on Cyber Resilience.

Amendment 53

Proposal for a regulation
Article 6 a (new)

Text proposed by the Commission	*Amendment*
	Article 6a
	Expert group on cyber resilience
	1. By ... [6 months after the date of entry into force of this Regulation], the Commission shall establish an expert group on cyber resilience (the 'Expert Group'). The composition of the Expert Group shall aim to be gender and geographically balanced and shall include the following:
	(a) representatives of each of the following:
	(i) the European Union Agency for Cybersecurity;
	(ii) the European Data Protection Board;
	(iii) Europol;
	(iv) the European Defence Agency;
	(b) experts representing relevant private stakeholders, ensuring adequate representation of micro, small and medium sized enterprises;
	(c) experts representing civil society, including consumer organisations;
	(d) experts appointed in a personal capacity, who have proven knowledge and experience in the areas covered by this Regulation;
	(e) experts representing academia, including universities, research institutes and other scientific organisations, including persons with global expertise.
	2. The Expert Group shall advise the

Commission with regard to the following:

(a) the list of critical products with digital elements set out in Annex III, as well as on the possible need to update that list;

(b) the implementation of European cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 and on the possibility to make them mandatory for highly critical products with digital elements;

(c) the elements of the Regulation to be addressed by the guidelines referred to in Article 17a;

(d) the availability and the quality of European and international standards, and the possibility to supplement or replace them with common technical specifications;

(e) the availability of skilled professionals in the field of cybersecurity across the Union, including of adequate personnel to perform third-party conformity assessments pursuant to this Regulation;

(f) the possible need to amend this Regulation.

The Expert Group shall also map trends at Union and Member State level regarding existing and patched vulnerabilities.

3. The Expert Group shall take into account the views of a wide range of stakeholders.

4. The Expert Group shall be chaired by the Commission and shall be constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. In that context, the Commission may invite experts with specific expertise on an ad hoc basis.

5. The Expert Group shall carry out its tasks in accordance with the principle

of transparency. The Commission shall publish a summary of the meetings of the Expert Group and other relevant documents on the Commission website.

Or. en

Justification

Stakeholder consultation will be essential to the functioning of this Regulation, which is why the Commission should create and consult extensively the Expert Group on Cyber Resilience.

Amendment 54

Proposal for a regulation
Article 9 a (new)

Text proposed by the Commission	*Amendment*
	Article 9a
	Public procurement of products with digital elements
	1. Without prejudice to Directives 2014/24/EU[1] and 2014/25/EU[2] of the European Parliament and of the Council, Member States shall ensure, when procuring products with digital elements, a high level of cybersecurity and appropriate expected product lifetimes.
	2. Member States shall ensure that manufacturers remedy vulnerabilities in publicly procured products with digital elements as a matter of urgency, including by making security updates available promptly.
	[1] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance (OJ L 94, 28.3.2014, p. 65).
	[2] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by

entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC Text with EEA relevance (OJ L 94, 28.3.2014, p. 243).

Or. en

Justification

It is essential that Member States prioritise cybersecurity in their public procurement.

Amendment 55

Proposal for a regulation
Article 10 – paragraph 4

Text proposed by the Commission	*Amendment*
4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements.	4. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements. ***When integrating components of open-source software that have not been placed on the market in the course of a commercial activity, manufacturers shall ensure that such components comply with this Regulation.***

Or. en

Amendment 56

Proposal for a regulation
Article 10 – paragraph 6 – subparagraph 1

Text proposed by the Commission	*Amendment*
When placing a product with digital elements on the market, ***and for*** the	When placing a product with digital elements on the market, ***manufacturers***

expected product lifetime ***or for a period of five years from the placing of the product on the market, whichever is shorter,*** manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.	***shall determine the expected product lifetime of those products. In doing so, the manufacturer shall ensure that*** the expected product lifetime ***is in line with reasonable consumer expectations and that it promotes sustainability and the need to ensure long-lasting products with digital elements.*** Manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I ***during at least the expected product lifetime***. ***Where applicable, the expected product lifetime shall be clearly stated on the product, its packaging or be included in contractual agreements.***

Or. en

Justification

The horizontal nature of this Regulation makes it difficult to set the expected product lifetime at a minimum or maximum period of years. Thus, the manufacturer should be able to set the expected product lifetime, provided that this is in line with consumer expectations and it is clearly advertised.

Amendment 57

Proposal for a regulation
Article 10 – paragraph 6 – subparagraph 2 a (new)

Text proposed by the Commission	*Amendment*
	Where applicable, for business-to-consumer products with digital elements, those procedures shall include automatic security updates by default. Users should retain the possibility of de-activating those automatic security updates.

Or. en

Justification

Where possible, security updates should be installed automatically.

Amendment 58

Proposal for a regulation
Article 10 – paragraph 6 – subparagraph 2 b (new)

Text proposed by the Commission	*Amendment*
	Manufacturers shall actively inform users when their product with digital elements has reached the end of its expected product lifetime and vulnerability handling requirements cease to apply.

Or. en

Amendment 59

Proposal for a regulation
Article 10 – paragraph 6 – subparagraph 2 c (new)

Text proposed by the Commission	*Amendment*
	Where the expected product lifetime is shorter than five years and the handling of vulnerabilities has therefore ended in accordance with the vulnerability handling requirements set out in Section 2 of Annex I, manufacturers shall provide free access to the source code of such a product with digital elements to undertakings. Those undertakings shall commit to extending the provision of vulnerability handling services, in particular security updates. Access to such source codes shall be provided only where provided for in a contractual arrangement. Those arrangements shall protect the ownership of the product with digital elements and shall prevent the dissemination of the source code to the public. The obligation to provide free access to the source code shall cease to apply when the lifetime of the product has reached five years.

Or. en

Amendment 60

Proposal for a regulation
Article 10 – paragraph 8

Text proposed by the Commission	*Amendment*
8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market.	8. Manufacturers shall keep the technical documentation and the EU declaration of conformity, where relevant, at the disposal of the market surveillance authorities for ten years ***or the expected product lifetime, whichever is longer,*** after the product with digital elements has been placed on the market.

Or. en

Amendment 61

Proposal for a regulation
Article 10 – paragraph 10 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Where such information and instructions are provided in electronic form, manufacturers shall:
	(a) present them in a user-friendly format that makes it possible for the user to consult them online, to download them, to save them on an electronic device and to print them;
	(b) ensure that they are accessible online during the expected lifetime of the product with digital elements.

Or. en

Justification

Information and instructions to users should be as user-friendly as possible.

Amendment 62

Proposal for a regulation
Article 10 – paragraph 12

Text proposed by the Commission	*Amendment*
12. From the placing on the market and for the expected product lifetime ***or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter***, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.	12. From the placing on the market and for the expected product lifetime, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.

Or. en

Justification

Necessary to align with the new definition of expected product lifetime.

Amendment 63

Proposal for a regulation
Article 10 – paragraph 15

Text proposed by the Commission	*Amendment*
15. The Commission ***may, by means of implementing acts,*** specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. ***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).***	15. The Commission ***is empowered to adopt delegated acts in accordance with Article 50 to*** specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I.

Or. en

Amendment 64

Proposal for a regulation
Article 11 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The manufacturer shall***, without undue delay and in any event within 24 hours of becoming aware of it,*** notify to ENISA any actively exploited vulnerability contained in the product with digital elements***. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken***. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of ***Directive [Directive XXX/XXXX (NIS2)]*** of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability.	1. The manufacturer shall notify to ENISA any actively exploited vulnerability contained in the product with digital elements ***in accordance with paragraph 1a of this Article***. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of ***Directive (EU) 2022/2555*** of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability. ***Where a notified vulnerability has no corrective or mitigating measures available, ENISA shall ensure that information about the notified vulnerability is shared in line with strict security protocols and on a need-to-know-basis.***

Or. en

Justification

The timetable for reporting and information to be included are aligned with NIS 2 (paragraph 1a). Secure protocols should be in place to ensure that information about unpatched vulnerabilities are not disseminated, to avoid further cybersecurity risks.

Amendment 65

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

Text proposed by the Commission	*Amendment*
	1a. Notifications as referred to in paragraph 1 shall be subject to the following procedure:
	(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the actively exploited vulnerability, detailing whether any known corrective or mitigating measure is available;
	(b) a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which, where applicable, updates the information referred to in point (a), details any corrective or mitigating measures taken and indicates an assessment of extent of the vulnerability, including its severity and impact;
	(c) an intermediate report on relevant status updates, upon the request of ENISA;
	(d) a final report, within one month after the submission of the vulnerability notification under point (b), including at least the following:
	(i) a detailed description of the vulnerability, including its severity and impact;
	(ii) where available, information concerning any actor that has exploited or that is exploiting the vulnerability;
	(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.

Or. en

Justification

Alignment with NIS 2.

Amendment 66

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

Text proposed by the Commission	*Amendment*
	1b. After a security update is made available or another form of corrective or mitigating measures is put in place, ENISA shall add the notified vulnerability pursuant to paragraph 1 to the European vulnerability database referred to in Article 12 of Directive (EU) 2022/2555.

Or. en

Justification

It is important that ENISA updates the vulnerability database with information about all known vulnerabilities that can be patched.

Amendment 67

Proposal for a regulation
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The manufacturer shall***, without undue delay and in any event within 24 hours of becoming aware of it,*** notify to ENISA any incident having impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of ***Directive [Directive XXX/XXXX (NIS2)]*** of the Member States concerned and inform the market surveillance authority about the notified incidents. The ***incident*** notification shall ***include information on the severity and impact of the incident and, where***	2. The manufacturer shall notify to ENISA any ***significant*** incident having impact on the security of the product with digital elements ***in accordance with paragraph 2b of this Article***. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of ***Directive (EU) 2022/2555*** of the Member States concerned and inform the market surveillance authority about the notified ***significant*** incidents. The ***mere act of*** notification shall ***not subject the notifying entity to increased liability***.

applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

Or. en

Justification

Only significant incidents should be reported on a mandatory basis, in alignment with NIS 2. Also the timetable needs alignment (par 2b).

Amendment 68

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

Text proposed by the Commission	*Amendment*
	2a. An incident shall be considered to be significant as referred to in paragraph 2, where:
	(a) it has caused or is capable of causing severe operational disruption of the production or the services for the manufacturer concerned, which would impact the security of a product; or
	(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Or. en

Justification

Alignment with NIS2 definition of significant incident. In order not to overburden manufacturers or ENISA too, only significant incidents affecting the security of the product should be reported on a mandatory basis.

Amendment 69

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

Text proposed by the Commission	*Amendment*
	2b. Notifications as referred to in paragraph 2 shall be subject to the following procedure:
	(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the significant incident, which, where applicable, indicates whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
	(b) an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the significant incident, which, where applicable, updates the information referred to in point (a) and indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
	(c) an intermediate report on relevant status updates upon the request of ENISA;
	(d) a final report, within one month after the submission of the incident notification under point (b), including at least the following:
	(i) a detailed description of the incident, including its severity and impact;
	(ii) the type of threat or root cause that is likely to have triggered the incident;
	(iii) applied and ongoing mitigation measures;
	(iv) where applicable, the cross-border impact of the incident;
	In the event of an ongoing incident at the time of the submission of the final report referred to in point (d) of the first subparagraph, Member States shall ensure that entities concerned provide a

progress report at that time and a final report within one month of their handling of the incident.

Or. en

Justification

Alignment with NIS 2.

Amendment 70

Proposal for a regulation
Article 11 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.	4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the ***significant*** incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the ***significant*** incident.

Or. en

Amendment 71

Proposal for a regulation
Article 11 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. ENISA shall ensure that notifications pursuant to paragraphs 1 and 2 are submitted via channels of communication and stored on servers that ensure the highest possible levels of cybersecurity and protection from malicious actors.

Or. en

Amendment 72

Proposal for a regulation
Article 11 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission ***may, by means of implementing acts,*** specify further the type of information, ***format and procedure*** of the notifications submitted pursuant to paragraphs 1 and 2. Those ***implementing*** acts shall be adopted ***in accordance with the examination procedure referred to in Article 51(2)***.	5. The Commission ***shall adopt delegated acts in accordance with Article 50 to*** specify further ***the format and procedure, as well as, where relevant,*** the type of information, of the notifications submitted pursuant to paragraphs 1 and 2. Those ***delegated*** acts shall be adopted ***by ... [12 months of entry into force of this Regulation]***.

Or. en

Amendment 73

Proposal for a regulation
Article 11 – paragraph 6

Text proposed by the Commission	*Amendment*
6. ENISA, on the basis of the notifications received pursuant to paragraphs 1 and 2, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article [Article X] of *Directive [Directive XXX/XXXX (NIS2)]*. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying.	6. ENISA, on the basis of the notifications received pursuant to paragraphs 1 and 2, shall prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group referred to in Article [Article X] of ***Directive (EU) 2022/2555***. The first such report shall be submitted within 24 months after the obligations laid down in paragraphs 1 and 2 start applying. ***ENISA shall include relevant information from its technical reports in its report on the state of cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555.***

Or. en

Amendment 74

Proposal for a regulation
Article 11 a (new)

Text proposed by the Commission	*Amendment*
	Article 11a
	Voluntary reporting
	1. In addition to the notification obligations set out in Article 11, notifications may be submitted to ENISA on a voluntary basis by the following:
	(a) manufacturers, with regard to incidents, cyber threats and near misses;
	(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Regulation, with regard to significant and non-significant incidents, cyber threats and near misses;
	(c) any actor with regard to vulnerabilities which may be included in the European vulnerability database referred to in Article 12 of Regulation 2022/255.
	2. ENISA shall process the notifications referred to in paragraph 1a of this Article in accordance with the procedure laid down in Article 11. ENISA may prioritise the processing of mandatory notifications over voluntary notifications.
	3. Where appropriate, ENISA shall ensure the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

Or. en

Amendment 75

Proposal for a regulation
Article 14 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.	3. Where a distributor considers or has reason to believe***, on the basis of information in their possession,*** that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.

Or. en

Justification

Distributors are often micro or SMEs. They should not be required to carry out proactive research into the conformity of products.

Amendment 76

Proposal for a regulation
Article 14 – paragraph 4 – subparagraph 1

Text proposed by the Commission	*Amendment*
Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity	Distributors who know or have reason to believe***, on the basis of information in their possession,*** that a product with digital elements, which they have made available on the market, or the processes put in place

with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.	by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate.

Or. en

Justification

Distributors are often micro or SMEs. They should not be required to carry out proactive research into the conformity of products.

Amendment 77

Proposal for a regulation
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. When the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.	6. ***On the basis of information in their possession,*** when the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

Or. en

Justification

Distributors are often micro or SMEs. They often do not know whether a manufacturer has ceased its operations.

Amendment 78

Proposal for a regulation
Article 17 a (new)

Text proposed by the Commission	*Amendment*
	Article 17a
	Guidelines
	1. In order to create clarity and certainty for and consistency among the practices of economic operators, the Commission shall prepare and issue guidelines in the form of a handbook for economic operators, explaining how to apply this Regulation, with a particular focus on how to facilitate compliance by micro, small and medium-sized enterprises.
	2. The guidelines shall be published by ... [12 months after the entry into force of this Regulation] and shall be regularly updated, in particular in light of potential amendments to the list of critical products set out in Annex III. They shall contain at least the following elements:
	(a) a detailed explanation of the scope of this Regulation, outlining the impact on the various sectors of the Union's economy;
	(b) clear and descriptive examples of remote data processing solutions designed and developed by or on behalf of the manufacturer ;
	(c) information to determine what constitutes a commercial activity for free and open-source software developers;
	(d) a detailed description of the methodology employed to distinguish between critical products with digital elements of classes I and II;
	(e) a clear illustration of the interaction between this Regulation and other Union law, particularly concerning presumptions of conformity and

conformity assessments;

(f) guidance for manufacturers on how to perform the cybersecurity risk assessment referred to in Article 10(2) and an explanation of how the risk assessment affects manufacturers' compliance with the essential requirements of this Regulation;

(g) guidance for manufacturers on how to determine appropriately the expected product lifetime, with an adequate level of product granularity;

(h) an explanation of how to handle reporting requirements pursuant to this Regulation or to other Union law;

(i) an overview of the Commission's empowerments to adopt delegated and implementing acts, with the relevant deadlines, where appropriate.

3. When preparing the guidelines pursuant to this Article, the Commission shall consult the Expert Group.

Or. en

Justification

This horizontal regulation presents a high degree of complexity, particularly for SMEs. The Commission should ensure comprehensive support to undertakings, including by providing them with guidelines and guidance on how to apply this Regulation.

Amendment 79

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
Where harmonised standards referred to in Article 18 do not exist or where the Commission ***considers that the relevant harmonised standards are insufficient to satisfy the*** requirements ***of this Regulation or*** to comply with the ***standardisation request of the Commission, or where there***	***1.*** The Commission ***is empowered to adopt delegated acts in accordance with Article 50 to establish common specifications that cover technical*** requirements ***providing a means*** to comply with the ***requirements set out in Annex I for products within the scope of this***

are undue delays in the standardisation procedure or where the ***request for harmonised standards by*** the Commission has ***not been accepted by the*** European standardisation organisations***, the Commission is empowered, by means of implementing acts, to adopt common specifications in respect of*** the essential requirements set out in Annex I***. Those implementing acts shall be adopted*** in accordance with ***the examination procedure referred to in Article 51(2)***.

Regulation where the ***following conditions have been fulfilled:***

(a) the Commission has ***requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more*** European standardisation organisations ***to draft a harmonised standard for*** the essential requirements set out in Annex I ***and the request has not been accepted or the European standardisation deliverables addressing that request is not delivered within the deadline set*** in accordance with ***Article 10(1) of Regulation (EU) No 1025/2012 or European standardisation deliverables do not comply with the request; and***

(b) no reference to harmonised standards covering the relevant essential requirements set out in Annex I is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.

2. Before preparing the delegated act, the Commission shall inform the Expert Group that it considers that the conditions in paragraph 1 are fulfilled. In preparing the delegated acts, the Commission shall take into account the opinions of the Expert Group.

3. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the publication of its reference in the Official Journal of the European Union, the Commission shall

assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference to a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the relevant delegated acts referred to in paragraph 1, or the parts thereof which cover the same essential requirements set out in Annex I.

Or. en

Justification

Common specifications should only be a last-resort option for the Commission. The text is broadly in alignment with the new General Product Safety Regulation.

Amendment 80

Proposal for a regulation
Article 20 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The EU declaration of conformity shall have the model structure set out in Annex IV and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VI. Such a declaration shall be continuously updated. It shall be made available in ***the*** language ***or languages required by*** the Member State in which the product with digital elements is placed on the market or made available.	2. The EU declaration of conformity shall have the model structure set out in Annex IV and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VI. Such a declaration shall be continuously updated. It shall be made available in ***a*** language ***which can be easily understood by the authorities of*** the Member State in which the product with digital elements is placed on the market or made available.

Or. en

Justification

It should be avoided that manufacturers of products with digital elements that often have a cross-border dimension are expected to prepare the declaration in 24 different languages.

Amendment 81

Proposal for a regulation
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, during the expected product lifetime ***or during a period of five years after the placing on the market of a product with digital elements, whichever is shorter***.	2. The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, during the expected product lifetime.

Or. en

Justification

Alignment with the new definition of expected product lifetime.

Amendment 82

Proposal for a regulation
Article 23 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by the elements to be included in the technical documentation set out in Annex V to take account of technological developments, as well as developments encountered in the implementation process of this Regulation.	5. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by the elements to be included in the technical documentation set out in Annex V to take account of technological developments, as well as developments encountered in the implementation process of this Regulation. ***The Commission shall ensure that the administrative burden on micro, small and medium sized enterprises is kept to a minimum.***

Or. en

Amendment 83

Proposal for a regulation
Article 24 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. Harmonised standards, common specifications or European cybersecurity certification schemes shall be in place for six months before the conformity assessment procedure referred to in paragraph 2 applies. In the six months prior to the application of paragraph 2, or where, due to a cause clearly attributable to the Commission, harmonised standards, common specifications or European cybersecurity certification schemes do not exist, manufacturers shall demonstrate the conformity of the critical product with digital elements of Class I as set out in Annex III via the procedure referred to in paragraph 1.

Or. en

Justification

Manufacturers of critical products of class I should not be penalised by the lack of harmonised standards, also in order to avoid an excessive recourse to third party conformity assessments, which could create bottlenecks and delay innovation. If harmonised standards, common specifications or European cybersecurity certification schemes are not available, or in the six months following their adoption, manufacturers may be able to demonstrate compliance with this Regulation via the self-assessment procedure.

Amendment 84

Proposal for a regulation
Article 24 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Notified bodies shall take into account the specific interests and needs of small and medium sized enterprises ***(SMEs)*** when setting the fees for conformity assessment procedures and	5. Notified bodies shall take into account the specific interests and needs of ***micro,*** small and medium sized enterprises when setting the fees for conformity assessment procedures and reduce those

reduce those fees proportionately to their specific interests and needs.	fees proportionately to their specific interests and needs. ***The Commission shall ensure appropriate financial support in the regulatory framework of existing Union programmes, in particular in order to ease the burden on micro, small and medium-sized enterprises.***

Or. en

Justification

It is key that the Commission puts in place financial support, to ease the compliance with this Regulation, particularly, for micro and SMEs.

Amendment 85

Proposal for a regulation
Article 24 a (new)

Text proposed by the Commission	*Amendment*
	Article 24a
	Mutual recognition agreements
	1. In order to promote international trade, the Commission shall endeavour to conclude Mutual Recognition Agreements (MRAs) with like-minded third countries. MRAs shall be established only between the Union and third countries that are on a comparable level of technical development and have a compatible approach concerning conformity assessment. They shall ensure the same level of protection as that provided for by this Regulation.
	2. The Commission shall assess international standards and evaluate whether they provide the same level of protection as the one provided for by this Regulation, with the aim to simplify the development of harmonised European standards.

Or. en

Amendment 86

Proposal for a regulation
Article 29 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7a. Member States and the Commission shall put in place appropriate measures to ensure sufficient availability of skilled professionals, in order to minimise bottlenecks in the activities of conformity assessment bodies.

Or. en

Amendment 87

Proposal for a regulation
Article 29 – paragraph 12

Text proposed by the Commission	*Amendment*
12. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, in particular taking into account the interests of ***SMEs*** in relation to fees.	12. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, in particular taking into account the interests of ***micro, small and medium-sized enterprises*** in relation to fees.

Or. en

Amendment 88

Proposal for a regulation
Article 41 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial ***and human*** resources to fulfil their tasks under	6. Member States shall ensure that the designated market surveillance authorities are provided with adequate financial resources ***and skilled personnel*** to fulfil

this Regulation.	their tasks under this Regulation.

Or. en

Amendment 89

Proposal for a regulation
Article 41 – paragraph 9 a (new)

Text proposed by the Commission	*Amendment*
	9a. Market surveillance authorities shall provide the Commission with data about the average expected product lifetime set by the manufacturers, disaggregated per category of product with digital elements. The Commission shall publish that information in a publicly accessible and user-friendly database.

Or. en

Amendment 90

Proposal for a regulation
Article 45 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it ***may*** request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.	1. Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it ***shall*** request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.

Or. en

Amendment 91

Proposal for a regulation
Article 45 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***may*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.	2. In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission ***shall*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.

Or. en

Amendment 92

Proposal for a regulation
Article 48 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Market surveillance authorities ***may agree with other relevant authorities to*** carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks.	1. Market surveillance authorities ***shall*** carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks.

Or. en

Amendment 93

Proposal for a regulation
Article 48 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission or ENISA ***may*** propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products falling in the scope of this Regulation with the requirements laid down by the latter.	2. The Commission or ENISA ***shall*** propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products falling in the scope of this Regulation with the requirements laid down by the latter.

Or. en

Amendment 94

Proposal for a regulation
Article 49 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Market surveillance authorities ***may decide to*** conduct simultaneous coordinated control actions (“sweeps”) of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation.	1. Market surveillance authorities ***shall regularly*** conduct simultaneous coordinated control actions (“sweeps”) of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation. ***Such sweeps shall prioritise products with digital elements placed on the market by manufacturers that maypresent a security risk for the Union. They shall include inspections of products acquired under a cover identity and shall aim to verify the compliance of those products with this Regulation, in particular with regard to identifying potential embedded backdoors or other exploitable vulnerabilities.***

Or. en

Justification

It is important to place a specific focus on manufacturers that can present cybersecurity risks to the integrity of the Union.

Amendment 95

Proposal for a regulation
Article 49 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep ***may, where appropriate,*** make the aggregated results publicly available.	2. Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep ***shall*** make the aggregated results publicly available.

Or. en

Amendment 96

Proposal for a regulation
Article 49 – paragraph 3

Text proposed by the Commission	*Amendment*
3. ENISA ***may*** identify, in the performance of its tasks, including based on the notifications received according to Article 11(1) and (2), categories of products for which sweeps ***may*** be organised. The proposal for sweeps shall be submitted to the potential coordinator referred to in paragraph 2 for the consideration of the market surveillance authorities.	3. ENISA ***shall*** identify, in the performance of its tasks, including based on the notifications received according to Article 11(1) and (2), categories of products for which sweeps ***shall*** be organised. The proposal for sweeps shall be submitted to the potential coordinator referred to in paragraph 2 for the consideration of the market surveillance authorities.

Or. en

Amendment 97

Proposal for a regulation
Article 49 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Market surveillance authorities ***may*** invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.	5. Market surveillance authorities ***shall*** invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.

Or. en

Amendment 98

Proposal for a regulation
Article 50 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The power to adopt delegated acts referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article ***20(5) and*** Article 23(5) shall be conferred on the Commission.	2. The power to adopt delegated acts referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article ***10(15), Article 11(5), Article 19(1), Article 20(5),*** Article 23(5) ***and Article 53a*** shall be conferred on the Commission.

Or. en

Amendment 99

Proposal for a regulation
Article 50 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The delegation of power referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article ***20(5) and*** Article 23(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day	3. The delegation of power referred to in Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article ***10(15), Article 11(5), Article 19(1), Article 20(5),*** Article 23(5) ***and Article 53a*** may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power

following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

Or. en

Amendment 100

Proposal for a regulation
Article 50 – paragraph 6

Text proposed by the Commission	*Amendment*
6. A delegated act adopted pursuant to Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article ***20(5) and*** Article 23(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	6. A delegated act adopted pursuant to Article 2(4), Article 6(2), Article 6(3), Article 6(5), Article ***10(15), Article 11(5), Article 19(1), Article 20(5),*** Article 23(5) ***and Article 53a*** shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Or. en

Amendment 101

Proposal for a regulation
Article 53 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall lay down the rules on penalties applicable to infringements by economic operators of	1. Member States shall lay down the rules on penalties applicable to infringements by economic operators of

this Regulation and shall take all measures necessary to ensure that they are enforced. The penalties provided for shall be effective, proportionate and dissuasive.	this Regulation and shall take all measures necessary to ensure that they are enforced. The penalties provided for shall be effective, proportionate and dissuasive***. They shall ensure that those rules take into account the financial capabilities of micro, small and medium-sized enterprises***.

Or. en

Amendment 102

Proposal for a regulation
Article 53 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.	2. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them. ***The Commission shall ensure that those rules and measures are applied in a uniform and consistent manner across the Union.***

Or. en

Amendment 103

Proposal for a regulation
Article 53 a (new)

Text proposed by the Commission	*Amendment*
	Article 53a
	Allocation of the revenue from the penalties to support cybersecurity in the Union
	1. The revenue from the penalties referred to in Article 53(1) shall be allocated to projects raising the level of cybersecurity within the Union. Those

projects shall aim to:

(i) increase the number of skilled professionals in the field of cybersecurity;

(ii) enhance capacity-building for micro, small and medium-sized enterprises in order to enable them to better comply with this Regulation;

(iii) improve collective situational awareness of cyber threats;

(iv) develop tools to increase the resilience of Union undertakings to cyber-enabled intellectual property theft.

2. The revenue referred to in paragraph 1 shall be allocated to the Digital Europe Programme referred to in Article 6 of Regulation (EU) 2021/694. It shall be earmarked to improve the cybersecurity of the Union. It shall constitute externally assigned revenue in accordance with Article 21(5) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[1] and shall be implemented in accordance with the rules applicable to the Digital Europe Programme. It shall be considered to be a budgetary top-up and shall not be used to decrease the contribution from the Union budget.

3. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation concerning the modalities for the payment of the penalties referred to in Article 53.

---

[1] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom)

No 966/2012 (OJ L 193, 30.7.2018, p. 1).

Or. en

Amendment 104

Proposal for a regulation
Article 55 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Until ... [40 months after the date of entry into force of this Regulation], manufacturers may comply with the requirements of this Regulation on a voluntary basis. Where manufacturers comply with this Regulation with regard to their products with digital elements , they shall be considered also to comply with Delegated Regulation (EU) 2022/30.
	After … [40 months after the date of entry into force of this Regulation, the Commission shall repeal Commission Delegated Regulation (EU) 2022/30.

Or. en

Justification

In order to encourage early compliance with the CRA, a presumption of conformity with the Delegated Regulation pursuant to the Radio Equipment Directive should be granted.

Amendment 105

Proposal for a regulation
Article 56 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Every year when presenting the Draft Budget for the following year, the Commission shall submit a detailed assessment of ENISA's tasks under this Regulation as set out in Annex VIa and other relevant Union law and shall detail

	the financial and human resources needed to fulfil those tasks.

Or. en

Amendment 106

Proposal for a regulation
Article 57 – paragraph 2

Text proposed by the Commission	*Amendment*
It shall apply from [***24*** months after the date of entry into force of this Regulation]. However Article 11 shall apply from [***12*** months after the date of entry into force of this Regulation].	It shall apply from … [***40*** months after the date of entry into force of this Regulation]. However Article 11 shall apply from [***20*** months after the date of entry into force of this Regulation].

Or. en

Justification

Sufficient time should be provided to economic operators to adapt to this Regulation, in light of its horizontal nature, broad scope and complexity.

Amendment 107

Proposal for a regulation
Annex I – Part 1 – point 2

Text proposed by the Commission	*Amendment*
(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;	***deleted***

Or. en

Justification

Moved under point (3) - on the basis of the risk assessment

Amendment 108

Proposal for a regulation
Annex I – Part 1 – point 3 – point -a (new)

Text proposed by the Commission	*Amendment*
	(-a) be delivered without known exploitable vulnerabilities;

Or. en

Justification

As some vulnerabilities may present very low or no cybersecurity risk, the obligation to deliver products without known exploitable vulnerabilities should be risk-based.

Amendment 109

Proposal for a regulation
Annex I – Part 1 – point 3 – point a

Text proposed by the Commission	*Amendment*
(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state ***while retaining all security updates***;

Or. en

Amendment 110

Proposal for a regulation
Annex I – Part 2 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;	(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates***, installed automatically where applicable***;

Or. en

Amendment 111

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

Text proposed by the Commission	*Amendment*
8. the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates;	8. ***the expected product lifetime,*** the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates***, and, where possible and applicable, a notification of the end of security updates***;

Or. en

Amendment 112

Proposal for a regulation
Annex III – Part I – point 18

Text proposed by the Commission	*Amendment*
18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;	***deleted***

Or. en

Justification

Moved fully under class II - routers and modems are key for cybersecurity

Amendment 113

Proposal for a regulation
Annex III – Part I – point 22

Text proposed by the Commission	*Amendment*
22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);	22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC)***, industrial robots and their control systems, mobile machinery*** and supervisory control and data acquisition systems (SCADA);

Or. en

Amendment 114

Proposal for a regulation
Annex III – Part I – point 23 a (new)

Text proposed by the Commission	*Amendment*
	23a. Home automation systems;

Or. en

Justification

Home automation systems play a key role in citizens' houses and should thus be deemed as critical products.

Amendment 115

Proposal for a regulation
Annex III – Part I – point 23 b (new)

Text proposed by the Commission	*Amendment*
	23b. Private security devices.

Or. en

Justification

Security cameras or smart locks are essential to the safety of citizens and should thus be

deemed as critical products.

Amendment 116

Proposal for a regulation
Annex III – Part II – point 7

Text proposed by the Commission	*Amendment*
7. Routers, modems intended for the connection to the internet, and switches***, intended for industrial use***;	7. Routers, modems intended for the connection to the internet, and switches;

Or. en

Amendment 117

Proposal for a regulation
Annex III – Part II – point 14

Text proposed by the Commission	*Amendment*
14. Robot sensing and actuator components and robot controllers;	***deleted***

Or. en

Amendment 118

Proposal for a regulation
Annex VI – Part A – point 4 – point 4.2

Text proposed by the Commission	*Amendment*
4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market. The EU declaration of conformity shall identify the product with digital elements	4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market ***or the expected product lifetime, whichever is longer***. The EU declaration of

for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

Or. en

Amendment 119

Proposal for a regulation
Annex VI – Part B – point 9

Text proposed by the Commission	*Amendment*
9. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market.	9. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market ***or for the expected product lifetime, whichever is longer***.

Or. en

Amendment 120

Proposal for a regulation
Annex VI – Part C – point 3 – point 3.2

Text proposed by the Commission	*Amendment*
3.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	3.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market ***or for the expected product lifetime, whichever is longer***. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

Or. en

Amendment 121

Proposal for a regulation
Annex VI – Part H – point 5 – point 5.2 – paragraph 1

Text proposed by the Commission	*Amendment*
The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up.	The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market ***or for the expected product lifetime, whichever is longer***. The declaration of conformity shall identify the product model for which it has been drawn up.

Or. en

Amendment 122

Proposal for a regulation
Annex VI – Part H – point 6 – introductory part

Text proposed by the Commission	*Amendment*
6. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market, keep at the disposal of the national authorities:	6. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market ***or for the expected product lifetime, whichever is longer***, keep at the disposal of the national authorities:

Or. en

Amendment 123

Proposal for a regulation
Annex VI a (new)

Text proposed by the Commission	*Amendment*
	Capacity needs of the European Union Agency for Cybersecurity (ENISA)
	In order to fulfil its obligations under this Regulation and in order not to compromise existing obligations of the Agency under other Union law, the adequate staffing and financing of ENISA shall be ensured. Therefore additional tasks for ENISA under this Regulation shall be accompanied by additional human and financial resources. 8,5 additional full-time posts and corresponding additional appropriations will be needed to cover the additional tasks under this Regulation.

Or. en

EXPLANATORY STATEMENT

The Rapporteur strongly welcomes the Commission proposal to address cybersecurity deficiencies in hardware and software products. In 2021, the global cost of cybercrime has reached a staggering EUR 5.5 trillion. This phenomenon, coupled with the upward trend of digitalisation, calls on legislators to ensure that appropriate cybersecurity measures are in place to safeguard the interests of both consumers and industry.

On this note, the Rapporteur is pleased that the Commission has put forward an ambitious proposal, which will raise the overall level of cybersecurity in the Member States and the functioning of the internal market. A harmonised regulatory framework is necessary so that undertakings who operate in the Single Market can benefit from legal clarity, as well as to ensure that the Union can play a leading role in the definition of norms on cybersecurity on the global stage.

On the issue of the scope, the rapporteur agrees with the Commission's proposal to include all products with digital elements. This comprehensive approach would provide assurance of cybersecurity compliance throughout the value chain, improving the competitiveness and the attractiveness of products manufactured in the Union. It is nonetheless necessary to simplify the current wording and refer to directly and indirectly connectable products, while excluding spare parts designed solely for the repair process, which have been in the market before this Regulation is implemented. When it comes to open source software, the Rapporteur is aware of the need to safeguard this important source of innovation and has thus put forward an amendment to ensure that developers should not be expected to comply with this Regulation if they are not receiving any financial returns for their projects. Nonetheless, open source software supplied in the framework of a commercial activity should be covered, to ensure the cybersecurity of the Union's ecosystem.

While the vast majority of products with digital elements will only have to undergo self-assessment, critical products pursuant to Article 6 will be subject to third party assessment. On this issue, the Rapporteur believes that the Regulation should be improved by providing more clarity on how often the list set out in Annex III can be amended as well as the procedures to follow after a product has been added to this list. The latter is particularly important in order to provide undertakings with adequate time to adjust. Nonetheless, the Rapporteur believes that home automation systems and products that enhance private security, such as cameras and smart locks, should constitute critical products under class I. This is because the integrity of these goods is paramount to citizens' safety and privacy.

Furthermore, the draft report foresees more involvement from stakeholders through the creation of the Expert group on Cyber Resilience. This body should be tasked to advise the Commission and to take an active role in the preparation of the delegated acts referred to in this Regulation. Thus, in order to express fully the interests of all side, the Expert group should be comprised of institutions, industry, civil society, academia and individual experts.

In addition to the aforementioned topic, the draft report stresses the need for Member States to take cybersecurity strongly into account when publicly procuring products with digital elements, and to ensure that vulnerabilities are promptly tackled.
On the issue of manufacturers' obligations, the rapporteur believes that having a set date for

the expected product lifetime is inadequate to a horizontal regulation, which intends to cover a wide range of products from software to phones and industrial machineries. This is why the rapporteur believes that it is more appropriate to have manufacturers determine the lifetime of their respective products, provided that the suggested duration is compatible with reasonable consumer expectations. A flexible duration would also enable manufacturers to showcase their products and have lengthy lifetimes as an element of competitiveness. Therefore, in order to raise the awareness of the consumers to this particular matter, the regulation should also oblige the manufacturers to clearly state the expected product lifetime on its packaging or include it in contractual agreements, and to notify the consumers when the lifetime is about to end. Furthermore, the draft report wants to put the utmost emphasis on safety. Thus, the rapporteur believes that the manufacturers should also be obliged to automatically update, when possible, safety features of their respective product. Where a manufacturer has defined an expected lifetime of under five years, it should stand ready to enter into contractual arrangements with undertakings that wish to provide services that extend a product's lifetime and disclose to them its source code. This possibility should not entail a transfer of ownership or the public disclosure of the source code.

On the matter of reporting obligations pursuant to Article 11, the Rapporteur wishes to align the timeline to the NIS2 so that there is more coherence and legal certainty for the stakeholders. In this sense, the Rapporteur suggests to report significant incidents (rather than all incidents), as well as actively exploited vulnerabilities, provided that clear protocols on how to handle such notifications securely are in place, as to avoid the spread of information concerning unpatched vulnerabilities. The Rapporteur also introduces a mechanism of voluntary reporting for other incidents, near misses and cyber threats.

However, to maximise the effect of reporting it is important to have a one-stop entity, also in order to simplify the reporting requirements for manufacturers across the Union. On this note, the Rapporteur believes that the best institution to play this role is ENISA. Therefore, in light of the increase in tasks and competence bestowed to ENISA, the Commission should modify the legislative financial statement accompanying this Regulation by providing the European Union Agency for Cybersecurity with additional posts and corresponding additional appropriations in order to fulfil the agency's additional tasks set out in this Regulation.

Additionally, an issue that is fundamental for the Rapporteur is to ensure that sufficient support is in place for undertakings to implement the requirements of this Regulation. This is particularly the case for micro, small and medium enterprises, which given their limited capabilities may find some challenges in ensuring compliance with the CRA. Therefore, the rapporteur believes that it is essential to prolong the date from which the regulation applies to 40 months. In this transition period, it should be possible for manufacturers to comply with the CRA on a voluntary basis, in order to obtain a presumption of conformity with the Radio Equipment Directive Delegated Regulation and to adapt to this Regulation ahead of its official implementation. Furthermore, the Rapporteur wants to emphasise the importance for the Union to provide support for the upskilling and reskilling of workers and ensure the availability of cybersecurity professionals, a key element for the success of this Regulation.

Moreover, as a general approach to help all stakeholders, the rapporteur calls for guidelines from the Commission to provide more specification on the actual implementation phase, thus providing more clarity to all parties involved.

Another equally pressing affair to the Rapporteur is international trade. This is why the draft report calls for the Commission to consider mutual recognition agreements with likeminded third countries, where they share comparable level of technical development and have a compatible approach concerning conformity assessment, ensuring the same level of protection as the one provided for by this Regulation. Nonetheless, it is essential that adequate monitoring of products coming from risky countries, which may contain backdoors or other vulnerabilities, is ensured: ENISA should coordinate with market surveillance authorities and perform the necessary checks on vendors who might present a higher risk profile.

Lastly, the rapporteur believes that revenues generated from the penalties should be earmarked to projects, which will raise the overall cybersecurity level across the Union, and hence be allocated to the Digital Europe Programme, supporting projects aimed at - among others - the re-skilling and upskilling of the current workforce.

ANNEX: LIST OF ENTITIES OR PERSONS FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT

Entity and/or person
(ISC)2
ACEM
Airlines4Europe
Alliance for IoT and Edge Computing Innovation
Amazon
American Chamber of Commerce
ANEC
Apple
APPLiA
Associazione Italiana Internet Provider
BDI
Beuc
Bitkom
BritCham
Broadcom
BSA - The Software alliance
Business Europe
Card Payment Sweden
CEMA
Centrum für Europäische Politik
CNH
Confederation of Danish Industries (DI)
Confindustria
Cybersecurity Coalition
DEKRA
Deutsche Telekom
Developers Alliance
Digital Europe
Enedis
Engineering
Ericsson
ESMIG
ETNO
ETRMA
European Cybersecurity Organisation
European Materials Handling Federation (FEM)
Eurosmart
Federunacoma
Free Software Foundation Europe
German Insurance Association
Giesecke+Devrient
GitHub

Google
GSMA
Hanbury Strategy
Huawei
IBM
Independent Retail Europe
Information Technology Industry Council
Leaseurope
Lenovo
Mechanical Engineering Industry Association (VDMA)
MedTechEurope
Microsoft
Okta
Open Forum Europe
Orange
Orgalim
Permanent Representation of Belgium
Permanent Representation of Italy
Permanent Representation of the Netherlands
Piaggio
Privacy International
SAP
Schneider Electric
Siemens
SME United
Splunk
Technology Industries of Finland
Telefonica
TIC Council
Trellix
Twillio
Unife
Vodafone Group
Wikimedia
Worldr
Xiaomi
Zoom