Table of Contents

BELGIUM 1
DENMARK 5
GERMANY 12
ITALY 23
FRANCE 33
LATVIA 35
THE NETHERLANDS 38
FINLAND 45

BELGIUM

Belgium's Written Comments on "Blocks 3 & 4" of the Cyber Resilience Act

Block 3 : Conformity

	Comments	Amendment suggestions (if any)
Art. 22 - Rules and conditions for affixing the CE marking **§1**	The Presidency compromise text for Art. 22(1) are removed the reference to the **website accompanying software products**. Although we understand that accompanying documents MAY be provided in digital format, we believe that this **should be a requirement,** not only an option. This is a guarantee that information is available to the customer before the purchase is completed.	1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to **~~the packaging and~~the accompanying documents and where applicable to the packaging ~~EU declaration of conformity referred to in Article 20 accompanying the product with digital elements.~~ For products with digital elements which are in the form of software, the CE marking shall be affixed ~~either~~ to the EU declaration of conformity referred to in Article 20 ~~or~~and on the website accompanying the software product**.
Art. 23 -	Belgium supports the removal of the reference to the 5-year period	2. The technical documentation shall be drawn up before the

Technical documentation **§2 & §4**	proposed by the European Commission in Art.23(2) in the Presidency compromise text. However, we think **the phrase "during the expected product lifetime" should be re-instated** to ensure legal certainty for manufacturers and avoid the impression of an indefinite period of time.	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.**~~
	As in the case of Annex II on Information and instructions to the user, it is important that the technical documentation be drafted **in clear and comprehensible terms**. Moreover, as in the case of Art. 22(1), we think the CRA should **require and not only allow the technical documentation to be provided online/in digital form.**	4. The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up **in clear and comprehensible terms,** in an official language of the Member State in which the notified body is established or in a language acceptable to that body. **4a. The technical documentation shall be available in an online medium and a permanent link to access the latest version shall be included in the user instructions.**
Annex IV – EU Declaration of Conformity	To support the idea of an "informed buyer", Belgium recommends **extending the contents of the declaration of conformity so that it clarifies aspects such as the intended use of the product, the applicable class (if Annex III is maintained) and the URL where details can be found on the vulnerability management**.	The EU declaration of conformity referred to in Article 20, shall contain all of the following information: 1. Name and type and any additional information enabling the unique identification of the product with digital elements; 2. Name and address of the manufacturer or his authorised representative; 3. A statement that the EU declaration of conformity is issued

		under the sole responsibility of the provider; 4**a.** Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate); **4b. The intended use of the product and the Class (as per Annex III) to which the product belongs**; 5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation; 6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared**, where applicable**; 7**a**. **The conformity assessment procedure applied (as per Annex VI), and w**here applicable, the name and number of the notified body~~**, a description of the conformity assessment procedure performed**~~ and identification of the corresponding certificate issued; **7b. The URL where the customer can gain access to relevant information on the vulnerability management procedure for the product;** 8. Additional information: […]

Block 4 : Market surveillance

Belgium has no amendment suggestions on Block 4, our remarks on Art. 29 (separation between role as notified body and other activities) and Art. 37 (appeals procedure) having been taken into account in the Presidency compromise text.

DENMARK

DK comments – Proposal for a Cyber Resilience Act (COM (2022) 454)

We continue to appreciate the considerable work, well-structured process and ambitious approach taken by the Presidency on the proposal thus far. We find that the text is still moving it in the right direction.

Below you will find our comments and suggestions for amendments. Our previous comments continue to be valid and the most important ones have been repeated here.

BLOCK III

Article 6 + Annex III – Critical Products

We continue to have serious concerns about the chosen approach to distinguish levels of criticality to a set of specific products. We find this approach to be contrary to the objectives of establishing a horizontal set of minimum cybersecurity requirements and detrimental to achieving it. Therefore, **we prefer to delete Article and Annex III**.

However, if kept in, we propose the following clarification, to avoid unnecessarily expanding the number of critical products significantly:

Article 6

Critical products with digital elements ***and highly critical products with digital elements***

1. **[**Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as ~~**falling in**~~ **belonging to** that category.**]**

   Categories of critical products with digital elements ~~**shall be**~~ **are** divided into class I and class II as set out in Annex III~~**, reflecting the level of cybersecurity risk related to these products.**~~ **The categories of products with digital elements listed in class I of Annex III meet one of the following criteria**:

   (a) the cybersecurity-related functionality of the product with digital elements, and in particular whether the primary function of that product is to perform ~~performs~~ functions critical to security, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;

Article 18 – Presumption of conformity

We continue to find it of high importance that there is a smooth interplay between this regulation and the certification schemes under the Cyber Security Act. We understand that it is the intention of Article 18. However, the process outlined in Article 18(4) seems unnecessarily cumbersome and could delay the implementation of both regulations and lead to unnecessary burdens for manufacturers.

We continue to propose the following amendments:

3. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 and specified as per paragraph 4, shall be presumed to be in conformity with the essential requirements set out in Annex I **and related conformity assessment procedures** in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements **at the relevant levels of assurance.**

4. ~~The Commission is empowered, by means of implementing acts, 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 thereof as set out in Annex I. Furthermore, where applicable, the Commission shall specify if a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).~~

Article 19 – Common specifications

As proposed before we continue to find it essential that this article is closely aligned with the compromise found in the machinery regulation. For ease of reference, please find below our suggested amendment, which was also submitted on the 3rd of February:

Article 19

Common specifications

~~**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 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).**~~

1. The Commission is empowered to adopt implementing acts, establishing common technical specifications for the essential cybersecurity requirements set out in Annex I, where the following conditions have been fulfilled:

(a) the Commission has requested, pursuant to Article 10(1) of Regulation 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the essential cybersecurity requirements set out in Annex 1 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 1025/2012 or European standardisation deliverables does not comply with the request, and

(b) no reference to harmonised standards covering the relevant essential cybersecurity requirements set out in Annex 1 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.

(c) Those implementing acts shall be adopted in accordance with the examination procedure referred to in article 51 (2).

2. Before preparing a draft implementing act, the Commission shall inform the committee referred to in Article 22 of Regulation EU (No) 1025/2012 that it considers that the conditions in paragraph 1 are fulfilled.

3. In the early preparation of the draft implementing act establishing the common specification, the Commission shall gather the views of relevant bodies or expert groups established under relevant sectorial Union law. Based on that consultation, the Commission shall prepare the draft implementing act.

4. When references of a harmonised standard are published in the Official Journal of the European Union, implementing acts referred to in paragraph 1, which cover the requirements set out Annex I, shall be repealed.

5.	**When a Member State considers that a common specification does not entirely satisfy the requirements set out in Annex I, it shall inform the Commission thereof with a detailed explanation and the Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification in question.**
6.	**Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify in the technical documentation referred to in Article 23 that they have adopted technical solutions that are at least equivalent thereto.**

BLOCK IIII

Article 7-9 - General Product Safety, High-risk AI systems, Machinery products

We do not find that the current recital 18 adequately covers the exemption of the eIDAS regulation, as more products than just European Digital Identity Wallets may be covered by both regulations.

We continue to propose the following amendments:

(18)	To the extent that their products fall within the scope of this Regulation and ~~, issuers of European Digital Identity Wallets as referred to in Article [Article 6a(2) of~~ Regulation (EU) No 910/2014, as amended by Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity], these products should comply with both the horizontal essential requirements established by this Regulation and the specific security requirements established by ~~Article [Article 6a of~~ Regulation (EU) No 910/2014, as amended by Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity]. ~~In order to facilitate compliance, wallet issuers should be able to demonstrate the compliance of European Digital Identity Wallets with the requirements set out respectively in both acts by certifying their products under a European cybersecurity certification scheme established under Regulation (EU) 2019/881 and for which the Commission specified via implementing act a presumption of conformity for this Regulation, in so far as the certificate, or parts thereof, covers those requirements.~~

Article 39 & 40 – Exchange of experience & Coordination of notified bodies

We continue to find it very important that national market surveillance authorities exchange knowledge and coordinate. We would like to see these articles strengthened, and find it important to ensure, that the national authorities have access to the needed cybersecurity expertise.

We propose a new article 40a, which could be modelled after article 68a in the AI general approach, but where the request could be made by the ADCO referred to in article 41(11). Furthermore, it could be considered if ENISA could play a role in this regard. We are open to discuss other suggestions however.

(NEW) Article 40a

Central pool of independent experts

1. Upon request of the ADCO referred to in article 41.11, the Commission shall, by means of an implementing act, make provisions on the creation, maintenance and financing of a central pool of independent experts to support the enforcement activities under this Regulation.
2. Experts shall be selected by the Commission and included in the central pool on the basis of up-to-date scientific or technical expertise in the field of cybersecurity, having due regard to the technical areas covered by the requirements and obligations in this Regulation and the activities of market surveillance authorities pursuant to Article 11 of Regulation (EU) 1020/2019. The Commission shall determine the number of experts in the pool in accordance with the required needs.
3. Experts may have the following tasks:
    a. provide advice to and support the work of market surveillance authorities, at their request;
    b. support cross-border market surveillance investigations, without prejudice of the powers of market surveillance authorities
    c. advise and support the Commission when carrying out its duties in the context of the safeguard clause pursuant to Article 44.

Article 50 & 51 – Exercise of the delegation & Committee procedure

As previously mentioned, we would prefer if the Commission was given competence to adopt implementing acts rather than delegated acts. If delegated acts must be maintained for legal reasons, the delegations should be specified and narrowed down in the relevant articles, as in the general approach on the AI Act.

Other comments

Finally, it seemed that our suggestion for a new recital 13a regarding tractors had not been received by the new presidency.

Regulation (EU) No 167/2013 establishes the requirements for the approval and market surveillance of agricultural and forestry vehicles. Vehicles with digital elements to which that Regulation applies are also subject to the CRA.

The CRA includes references to legislation where vehicles are either included or exempted from the scope of application. This includes the reference to Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users and to the Machinery Regulation, recital 30 and Article 9.

We would like to get a clarification on whether two- or three-wheel vehicles and quadricycles are also subject to the CRA. If these vehicles are indeed subject to the regulation, we suggest including Regulation 168/2013 in a new recital.

There is a need for further clarification in the recitals to avoid misunderstandings regarding which vehicles with digital elements are subject to this proposed Regulation.

We suggest the following clarifying Recital 13 a on the scope of application as regards the above mentioned vehicles:

(13a) Regulation (EU) No 167/2013 of the European Parliament and of the Council establishes the requirements for the approval and market surveillance of agricultural and forestry vehicles and Regulation (EU) No 168/2013 of the European Parliament and of the Council establishes the requirements for the approval and market surveillance of two- or three-wheel vehicles and quadricycles. Vehicles to which either of those Regulations apply with digital elements are subject to this Regulation.

GERMANY

BLOCK 3

Article 6

Critical products with digital elements ***and highly critical products with digital elements***

1. **[**Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as ~~**falling in**~~ **belonging to** that category.**]**

   Categories of critical products with digital elements ~~**shall be**~~ **are** divided into class I and class II as set out in Annex III~~**, reflecting the level of cybersecurity risk related to these products.**~~ **The categories of products with digital elements listed in class I of Annex III meet one of the following criteria**:

   (b) the cybersecurity-related functionality of the product with digital elements, and in particular whether that product performs functions critical to security, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;

   (c) the product with digital elements performs a central system function, including network management, configuration control, virtualisation, processing of personal data, or functions having the potential to disrupt, control or damage a large number of other products with digital elements through direct manipulation or having the potential of an adverse impact in particular in terms of its intensity and its ability to affect a plurality of persons..

   The categories of products with digital elements listed in class II of Annex III meet at least two of the following criteria:

   (a) the criteria referred to in the second subparagraph, point (a);

   (b) the criteria referred to in the second subparagraph, point (b);

   (c) the intended ~~**use**~~ **application of the product with digital elements** in sensitive environments[1], including in industrial **control** settings ~~**or**~~ **and** by ~~**essential**~~ entities of ~~**the**~~ **a** type referred to in ~~**the**~~ Annex **I** to ~~**the**~~ Directive **(EU) 2022/2555** ~~**[Directive XXX:XXXX (NIS2)]**~~**.**

2. **[**The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list **within each class** of **the** 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 **referred to in paragraph 1 of this Article** shall be taken into account~~.~~:

   ~~**(a) the cybersecurity-related functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:**~~

   ~~**(i) it is designed to run with elevated privilege or manage privileges;**~~

   ~~**(ii) it has direct or privileged access to networking or computing resources;**~~

   ~~**(iii) it is designed to control access to data or operational technology;**~~

[1] Possible recital

~~(iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection.~~

~~(b) the intended use in sensitive environments, including in industrial settings or by essential entities of the type referred to in the Annex [Annex I] to the Directive [Directive XXX/XXXX (NIS2)];~~

~~(c) the intended use of performing critical or sensitive functions, such as processing of personal data;~~

~~(d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;~~

~~(e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact.~~]

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].]

4. Critical products with digital elements shall be subject to the conformity assessment procedures referred to in Article 24(2) and (3).

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 **at assurance level 'substantial' or 'high'** 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. Such implementing acts shall be adopted by the Commission as soon as demand for such acts arises. When determining such categories of highly critical products with digital elements, the Commission shall take into account **the criteria referred to in paragraph 1 of this Article** ~~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~~ **any of the following criteria**:

   (a) ~~used or~~ **the extent to which there is a critical dependency of entities of a type referred to in Annex I to ~~the~~ Directive (EU) 2022/2555 on the category of products with digital elements ~~relied upon byof the essential entities of a the type referred to in Annex [Annex I] to the Directive (EU) 2022/2555 [Directive XXX/ XXXX (NIS2)]~~ ~~or~~ ~~will have potential future significance for the activities of these entities; or~~**

   (b) intended for essential energy system functions such as balancing, dispatch, redispatch and congestion management, collection or processing of grid status information by system operators, aggregation or smart and bidirectional charging of mobile or stationary batteries; or

   (c) ~~relevant for the resilience of the overall~~ **the extent to which cybersecurity incidents and exploited vulnerabilities concerning the category of products with digital elements can lead to** disruptive events[2] **for critical** supply chains ~~of products with digital elements against disruptive events~~ **across the internal market.]**

[2] A recital may be added.

Article 18
Presumption of conformity

1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with the essential requirements covered by those standards or parts thereof, set out in Annex I.
2. Products with digital elements and processes put in place by the manufacturer, which are in conformity with the common specifications referred to in Article 19 shall be presumed to be in conformity with the essential requirements set out in Annex I, to the extent those common specifications cover those requirements.
3. Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 and specified as per paragraph 4, shall be presumed to be in conformity with the essential requirements set out in Annex I **and related conformity assessment procedures** in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.
4. The Commission is empowered, by means of implementing acts, 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 thereof as set out in Annex I. Furthermore, ~~**where applicable,**~~ the Commission shall specify ~~**if**~~ **for which assurance levels,** a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

Article 19
[Common specifications][3]

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 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).

[3] Will be updated according to Art 17 in the Machinery Regulation once it is finalised.

Article 22
Rules and conditions for affixing the CE marking

6. The Commission may, by means of implementing acts, 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

[ANNEX III

CLASSES AND CATEGORIES OF CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class I

Categories of products with digital elements which meet the criteria referred to in Article 6(1), second subparagraph, point (a):

~~**1. Identity management systems software and privileged access management software;**~~
~~**2. Standalone and embedded browsers;**~~

~~**3. Password managers;**~~

1. ~~**4.**~~Software that searches for, removes, or quarantines malicious software;
~~**5. Products with digital elements with the function of virtual private network (VPN);**~~
~~**6. Network management systems;**~~
~~**7. Network configuration management tools;**~~
2. ~~**8.**~~Network traffic monitoring systems **for throughput and flow control**;
~~**9. Management of network resources;**~~
3. ~~**10**~~. Security information and event management (SIEM) systems;
4. ~~**11.**~~ **Update**/patch management, including boot managers;
5. ~~**17.**~~ Firewalls, intrusion detection and/or prevention systems not covered by class II;
6. ~~**3.**~~ **Public key infrastructure and digital certificate issuersance software;**
7. Smart home products with safety functionalities, such as door locks and alarm systems.

8. Wearable technology and other connected health devices

9. Connected products intended for use by and for children (including toys and baby monitors)
~~**12. Application configuration management systems;**~~
~~**13. Remote access/sharing software;**~~
~~**14. Mobile device management software;**~~
~~**15. Physical network interfaces;**~~

Categories of products with digital elements which meet the criteria referred to in Article 6(1), second subparagraph, point (b):

8. ~~16.~~Operating systems not covered by class II;
~~**17. Firewalls, intrusion detection and/or prevention systems not covered by class II;**~~
9. ~~2.~~ Standalone and embedded browsers;
10. ~~9.~~Management of network resources**, including software-defined networking (SDN) technology;**
11. ~~12.~~Application configuration management systems **for centralised systems configuration;**
12. ~~13.~~ Remote access/sharing software;
13. ~~14.~~ Mobile device management software **for the configuration, monitoring and updating of mobile devices;**
14. ~~15.~~ Physical **and virtual** network interfaces;
15. ~~18.~~ Routers, modems intended for the connection to the internet, and switches, not covered by class II;
16. ~~19.~~ Microprocessors ~~**not covered by class II,**~~ including general purpose microprocessors;
17. ~~20.~~ Microcontrollers;
~~**21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];**~~
18. ~~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);
19. ~~23.~~Industrial Internet of Things not covered by class II**;**
20. ~~14. Robot sensing and actuator components and~~ Industrial robot controllers.

Class II

Categories of products with digital elements which meet both the criteria referred to in Article 6(1), third subparagraph, points (a) and (b):

~~**1. Operating systems for servers, desktops, and mobile devices**~~;
1. Identity management systems software and privileged access management software;
2. Authentication tools; ~~Password managers~~
3. Products with digital elements with the function of virtual private network (VPN);
4.~~ 6.~~ Network management systems for the configuration, monitoring and updating of network devices;
~~5. 2.~~ Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
~~**3.Public key infrastructure and digital certificate issuers;**~~
~~**4.Firewalls, intrusion detection and/or prevention systems intended for industrial use;**~~
~~**5.General purpose microprocessors;**~~
6. Microprocessors intended for integration in programmable logic controllers and secure elements;
~~**7.Routers, modems intended for the connection to the internet, and switches, intended for industrial use;**~~
6. 8~~.~~ Devices based on tamper-resistant integrated circuits, including embedded and integrated Ssecure Eelements;
7.~~ 9.~~ Hardware Security Modules (HSMs);
8. ~~10.~~ Secure cryptoprocessors;
9. ~~11.~~ Smartcards, smartcard readers and tokens.
Categories of products with digital elements which meet both the criteria referred to in Article 6(1), third subparagraph, points (a) and (c):
10. 4. Firewalls, intrusion detection and/or prevention systems intended for industrial use**.**

Categories of products with digital elements which meet both the criteria referred to in Article 6(1), third subparagraph, points (b) and (c):

~~**8. Secure elements;**~~

~~**9. Hardware Security Modules (HSMs);**~~
~~**10. Secure cryptoprocessors;**~~
~~**11. Smartcards, smartcard readers and tokens;**~~
11.~~ 21.~~ Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
12. Industrial Automation & Control Systems (IACS) **and components** intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], 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);
13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
~~**14. Robot sensing and actuator components and robot controllers;**~~
14. ~~15.~~ Smart meters **as defined in Article 2(23) of Directive (EU) 2019/944.]**

ANNEX [XX]
Simplified EU declaration of conformity

The simplified EU declaration of conformity referred to in Article [10(11)] shall be provided as follows:

Hereby, [Name of manufacturer] declares that the product with digital elements type [designation of type of product with digital element] is in compliance with Regulation XX.
The full text of the EU declaration of conformity is available at the following internet address:

BLOCK 4

Article 9

Machinery products

Machinery products under the scope of Regulation [Machinery Regulation proposal] which are products with digital elements within the meaning of this Regulation ~~and for which an EU declaration of conformity has been issued on the basis of this Regulation~~ shall be deemed to be in conformity with the **requirements related to cybersecurity regarding the protection against corruption and safety and reliability of control systems** ~~essential health and safety requirements~~ set out in **Sections 1.1.9 and 1.2.1 of** Annex [Annex III, ~~Sections 1.1.9 and 1.2.1~~] to Regulation [Machinery Regulation proposal], ~~as regards protection against corruption and safety and reliability of control systems, and in so far as~~ **if** the achievement of the level of **cybersecurity** protection required ~~by~~ **under** those ~~requirements~~ **Sections** is demonstrated in the EU declaration of conformity issued ~~under~~ **pursuant to** this Regulation.

CHAPTER IV

NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

Article 26

Notifying authorities

1. Member States shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, including compliance with Article 31.

2. Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with Regulation (EC) No 765/2008.

3. Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 to a body which is not a governmental entity, that body shall be a legal entity and shall comply mutatis mutandis with the requirements laid down in [Article 27] of this Regulation. In addition it shall have arrangements to cover liabilities arising out of its activities.

4. The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3.

Article 30

Presumption of conformity of notified bodies

Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* it shall be presumed to comply with the requirements set out in Article 29 in so far as the applicable harmonised standards cover those requirements.

CHAPTER V

MARKET SURVEILLANCE AND ENFORCEMENT

Article 42

Access to data and documentation

Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential requirements set out in Annex I and upon a reasoned request, the market surveillance authorities shall be granted access to the data required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the respective economic operator.

Article 43

Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk

1. Where the market surveillance authority of a Member State has sufficient reasons to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall carry out an evaluation of the product with digital elements concerned in respect of its compliance with ~~all~~ the requirements laid down in this Regulation. The relevant economic operators shall cooperate as necessary with the market surveillance authority.

Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant **economic** operator to take ~~all~~ appropriate corrective actions to bring the product **with digital elements** into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as ~~it~~ **the market surveillance authority** may prescribe.

The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the ~~appropriate~~ corrective actions.

CHAPTER VIII

TRANSITIONAL AND FINAL PROVISIONS

Article 54

Amendment to Regulation (EU) 2019/1020

In Annex I to Regulation (EU) 2019/1020 the following point is added:

’71. [Regulation XXX][Cyber Resilience Act]’.

Article 54 a)

Amendment to Regulation (EU) 2020/1828

In Annex 1 to Regulation (EU) 2020/1828 the following point is added:

’67. [Regulation XXX][Cyber Resilience Act]’.

ITALY

Italian National Cybersecurity Agency Comments on the Cyber Resilience Act

16 March 2023

These comments are without prejudice to further positions the Italian National Cybersecurity Agency or other national authorities may provide on this matter.

1 Scope

1.1 Exclusion clause

Concerning the exclusion clause (paragraph 5, article 2), our position is to rephrase the terms "developed exclusively for" into "intended for use of".
Moreover, concerning the latest Presidency compromise proposal, our position is to reintroduce the previously added paragraphs 5b and 5c of article 2, while supporting the addition of paragraph 5 of article 4.
Finally, we support the introduction of an additional paragraph safeguarding domestic jurisdiction. A possible phrasing could be as follows "Member State may adopt or maintain provision with a view to achieving a higher level of cybersecurity of products with digital elements".
As per the "maintaining" of existing provisions, art. 114.4 and 114.6 of the TFEU might apply. The mentioned articles provide for a judicial basis to such a purpose, on grounds of major needs referred to in Article 36 (among them, national security is mentioned).

As per the "adoption" of (additional) provisions, a similar framework is provided for in directive 1535/2015.

Amendments 1: Article 2.

5. This Regulation does not apply to products with digital elements ~~developed exclusively for~~**intended for use** of national security, defence or military purposes or to products specifically designed to process classified information.
5b. This Regulation is without prejudice to the Member States' responsibilities to safeguard national security or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.
5c. The obligations laid down in this Regulation do not entail the supply of information the disclosure of which is contrary to the Member States' essential interests of national security, public security or defence.
5d. Member States may adopt or maintain provision with a view to achieving a higher level of cybersecurity of products with digital elements.

1.2 Exclusion of non-connectable products with digital elements

As mentioned in our previous comments (WK 17303/2022), our position is to remove the scope limitation to only "connectable" products. That is, applying the Regulation to all products with digital elements independently from their capability to exchange data at the time of their placing on the market.
Therefore, paragraph 1 of article 2 would read as follows: "This regulation applies to product with digital elements". It greatly simplifies the text, making it future proof and less exposed to loopholes.

Amendments 2: Article 2, paragraph 1.

Article 2 *Scope* 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~~.

This would also entail the deletion of the now unnecessary definitions of "logical connection", "physical connection" and "indirect connection" (paragraphs 11, 12 and 13 of article 3).
Mind that, taking into consideration the principles of proportionality, this slight increase in the scope is counterbalanced by the simplification in the conformity assessment procedures, reduction of initial critical products and fine tuning of the essential requirements (see section 5).

1.3 Exclusion of services and software as a service

While a national position has not been finalized yet, we are sceptical on the exclusion of services from the scope of the Regulation (paragraph 1, article 3), with particular emphasis on Sofware-as-a-Service (recital 9).
In this regards, we do not see major differences in between the mentioned services and the "remote data processing" and have some concerns in the application of CRA on products that leverage SaaS services (who is responsible for what?).
The changes in the recital 9 in the latest Presidency compromise proposal are proceeding in the right direction but may not be sufficient.
Therefore, we would welcome additional explanations by the Commission as well as continuing the discussion on this topic in HWPCI and are inclined to support the position of those Member States asking for the full inclusion of services and SaaS in the scope of the Regulation.

1.4 Open source

Recital 10 clarifies that "only free and open-source software […] supplied in the course of a commercial activity and therefore placed on the market should be covered by this Regulation.".
While we agree with the overarching principle, we have two concerns with this provision:

1. inability for non-commercial open-source software to achieve the CE marking;
2. impact on the commercial services offered by companies that do not control most of the code-base of the non-commercial open-source software.

Concerning the former, we propose to introduce the possibility for non-commercial open-source software to undergo the conformity assessment to achieve the CE marking on a voluntary basis. This would also benefit:

- consumers that may therefore differentiate between open-source projects that are willing to undergo some scrutiny with respect to those that won't;
- open-source itself as its otherwise inability to achieve the CE marking may hamper its usage by consumer that may understandably associate the lack of CE marking as an indicator of untrustworthiness.

Concerning the latter, the current formulation (in combination with article 10, paragraph 4) may prevent the usage of open-source software in commercial product, as the companies that use open-source libraries or embed third-party open-source product would then be responsible to perform due diligence and ensure that the security of their product is not compromised by pieces of software they do not control and that are not subject to CRA requirements , which may not be technically feasible. This may in turn be a blow to innovation or research limiting the industrial usage of open-source.
We would welcome a discussion to address this issue.
A preliminary proposal to amend Article 24 is as follows:

Amendments 3: Article 24

4a.	**On a voluntary basis, for the purposes of applying the CE marking pursuant to article 22, products with digital elements not covered by this Regulation may demonstrate conformity with the essential requirements set out in Annex I by using any of the procedures referred to in paragraph 1.**

2 Interplay with other EU regulation

2.1 Interplay with Maritime and other sectoral regulations.

We would like to point out possible issues in the application of CRA with respect to products covered by Directive 2014/90 on marine equipment. We would therefore request a joint analysis on this topic by DG Connect, DG Move and DG Mare.
Generally speaking, we would welcome a broader analysis from the Commission to assess the impact of CRA with respect to EU legislation that tackles the concepts of conformity assessment and certification.

3 Reporting obligation

3.1 Notification process

Concerning the reporting obligation of manufacturer framework outline in article 11, the latest Presidency proposals (ST 5806/23 and WK 3408/23) did improve on the previous phrasing. Indeed, our position is that vulnerabilities and incident notification must be notified directly to the CSIRT or national cybersecurity authority of the relevant Member State(s). This would also allow to promptly activate the already existing structures for cross-border cooperation at technical level (CSIRT Network) and operational level (CyCLONe) without introducing any additional mechanism, while also providing the opportunity for synergies in the implementation of the CVD policy that must be developed at national level under NIS2.
This is without prejudice to a possible subsequent notification of vulnerabilities from the Member State to ENISA, as provided by NIS2 in the context of CVD.

However, we believe it is redundant to require the notification also to the Single Point of Contact, which is an additional burden on the manufacturer while the same effect can be easily achieve with appropriate coordination at governmental level.
Moreover, we propose the following additional amendments to Article 11:

- MS may derogate to ENISA the management of vulnerabilities [insertion of paragraph 1a];
- Article 11 should not apply to vulnerabilities under the process of the NIS2 CVD [insertion of paragraph 1b].

Finally, the last Presidency proposal (WK 3408/23) provides that the CSIRT Network submit notifications to EU-CyCLONe (Article 11(3)), instead of ENISA as in the previous formulation. We think that this is not appropriate for two main reasons:

- the cooperation between the CSIRT Network and EU-CyCLONe is established on the basis of procedural arrangements agreed upon by the two parties as provided by NIS 2 Directive (Articles 15(6) and 16(6)) and, therefore, this Regulation should not impose an exchange of information between these parties;
- this might possibly introduce delays in information flow to CyCLONe. Indeed, while the current formulation already requires national CSIRTs to forward notification to ENISA without undue delay (which in turn, as per the previous formulation, would submit the notification to EU-CyCLONe), there is currently no requirement for national CSIRTs to *promptly* forward notifications to the CSIRT Network.

Moreover, as the developer and maintainer of the European vulnerability database (pursuant to Article 12(2) of NIS 2 Directive), it is more natural that ENISA should be in charge of submitting notifications to EU-CyCLONe.

For these reasons, we propose to revert paragraph 3 of Article 11 to the previous formulation with regard to who is in charge to submit notifications to EU-CyCLONe.

Amendments 4: Article 11

Article 11

Reporting obligations of manufacturers

1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify **to the CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure** ~~**in accordance with**~~**pursuant to Article** ~~**[Article X]**~~ **12(1) of Directive** ~~**[Directive XXX/XXXX (NIS2)]**~~**(EU) 2022/2555 of Member States concerned [through a single reporting platform]** ~~**to ENISA**~~ any ~~actively exploited~~ vulnerability contained in the product with digital elements. The notification shall include **technical** details concerning that vulnerability

and, where applicable, any corrective or mitigating measures taken.

~~ENISA~~ **The CSIRTs** shall, without undue delay, unless for ~~justified~~ cybersecurity risk-related grounds, forward the notification to **ENISA** ~~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 authorities **of all the concerned Member States** ~~y~~ about the notified vulnerability.

1a. By way of derogation of the first paragraph, Member States may delegate to ENISA the management of notification under this article.

1b. If the manufacturer is already engaged in a coordinated vulnerability disclosure pursuant to Article 12(1) of Directive (EU) 2022/2555 of Member States concerned with respect to a vulnerability, this article does not apply to the concerned vulnerability.

~~2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA the single point of contact designated or established in accordance with pursuant to Article [Article X]8(3) of Directive (EU) 2022/2555 [Directive XXX/XXXX (NIS2)] of the Member States concerned [through a single reporting platform] any incident having impact on the security of the product with digital elements. ENISAThe designated single point of contact 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 ENISA and inform the market surveillance authorities in all concerned Member States about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where 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.~~

2a. For all products with digital elements, the manufacturer shall have the possibility for the voluntary reporting of vulnerabilities of which active exploitation have not yet been observed.

2b. In the case that a third party other than manufacturer discloses an actively exploited vulnerability or an incident of a product under the scope of this Regulation to the CSIRT, the CSIRT shall without undue delay inform the manufacturer.

3. ~~The EU-CSIRT-Network~~ **ENISA** shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established ~~by~~**under** Article ~~[Article X]~~**16** of Directive **(EU) 2022/2555** ~~[Directive XXX/XXXX (NIS2)]~~ information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

3.1 Notification scope

Concerning the events that should be notified, our position is that, in addition to exploited vulnerabilities and incidents, manufacturer should also notify discovered vulnerabilities (see previous box, paragraph 1, Article 11).

4 Essential Requirments

4.1 Vulnerabilities management timeframe

The "Non-paper on a support period covering the entire expected product lifetime in the Cyber Resilience Act" (WK 2942/2023) already provides our current position.
While the latest Presidency compromise proposal (WK 3408/2023) implemented the comments related to blocks 1-2 of the abovementioned non-paper, we support also the inclusion of the comments to the other blocks, notably the introduction of the following amendment to Article 41, providing for Market surveillance authorities to publish statistics on expected product lifetimes provided by manufacturers:

Amendments 5: Article 41

8a. Market surveillance authorities may publish statistics about the average expected product lifetime, as specified by the manufacturer pursuant to article 10 (10a), per category of products with digital elements..

5 Product criticality hierarchy, conformity assessment procedures and list of critical products.

The current framework defines four levels of criticality of products mapped to five "procedures" to demonstrate their conformity to the essential requirements (module A, module B+C or module H, harmonized standards, CSA).
The highly critical products mechanism introduces an ex-ante last resort option to cover non-anticipated situations, without resorting to the ex-post powers in article 45. Therefore, while the implementation may be improved, we are not against the underlying principle within the Regulation.
On the other hand, it may be argued that the distinction between noncritical, class I critical and class II critical products could be simplified and that three different procedures of conformity assessment reduce the differentiation in between the three levels.
It should also be considered that some categories in the critical product list are linked to their intended use for essential entities under NIS2. In our understanding, ensuring high level of cybersecurity within critical infrastructure should be handled under CSA (with certification) and

NIS2 (with security measures) as they consider the criticality of product based on their context of usage. On the other hand, CRA should be aimed at ensuring minimum cybersecurity considering the intrinsic criticality of a product from a horizontal standpoint. Therefore, we would argue that, while usage in critical infrastructure may be considered in the reasoning to identify critical products, it should not be the main factor.
Moreover, considering that the most impactful provision of the CRA is the ex-ante third-party conformity assessment rather than the requirements themselves and that the list of critical products may be updated in the future, it would be safer to limit the number of product categories listed in Annex II.
Therefore, we propose to:

1. apply class II conformity demonstration procedure provision to all critical products;
2. remove the class I and class II distinction within the critical product;
3. review the list of categories of critical product, from cumulatively 33 to roughly 10.

This approach would simplify the regulation, reducing the number of procedures and categories to be fine-tuned, while also avoid overloading the industry, the national authorities, and the notified bodies in the initial application of the CRA.
Therefore, we propose the following amendments to Article 6 and Article 24:

Amendments 6: Article 6.

Article 6

Critical products with digital elements ***and highly critical products with digital elements***

1. **[**Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as ~~**falling in**~~ **belonging to** that category.**]**

~~Categories of critical products with digital elements shall be are divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products.~~ **The categories of products with digital elements listed in ~~class I of~~ Annex III meet one of the following criteria**:

(d) the cybersecurity-related functionality of the product with digital elements, and in particular whether that product performs functions critical to security, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;

(e) the product with digital elements performs a central system function, including network management, configuration control, virtualisation, processing of personal data, or functions having the potential to disrupt, control or damage a large number of other products with digital elements through direct manipulation.

~~**The categories of products with digital elements listed in class II of Annex III meet at least two of the following criteria:**~~

~~**(a) the criteria referred to in the second subparagraph, point (a);**~~

~~**(b) the criteria referred to in the second subparagraph, point (b);**~~

~~(c) the intended use application of the product with digital elements in sensitive environments , including in industrial control settings or and by essential entities of the a type referred to in the Annex I to the Directive (EU) 2022/2555 [Directive XXX:XXXX (NIS2)].~~

2. [The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend Annex III by including in the list ~~within each class~~ of **the** 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 **referred to in paragraph 1 of this Article** shall be taken into account.~~:~~

~~**(a) the cybersecurity-related functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:**~~

~~**(i) it is designed to run with elevated privilege or manage privileges;**~~

~~**(ii) it has direct or privileged access to networking or computing resources;**~~

~~**(iii) it is designed to control access to data or operational technology;**~~

~~**(iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection.**~~

~~**(b) the intended use in sensitive environments, including in industrial settings or by essential entities of the type referred to in the Annex [Annex I] to the Directive [Directive XXX/XXXX (NIS2)];**~~

~~**(c) the intended use of performing critical or sensitive functions, such as processing of personal data;**~~

~~**(d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;**~~

~~**(e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact.]**~~

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].]

Amendments 7: Article 24.

Article 24

Conformity assessment procedures for products with digital elements

1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer ~~**or the manufacturer's authorised representative**~~ shall demonstrate conformity with the essential requirements by using ~~**one**~~ **any** of the following procedures:

   (a) the internal control procedure (based on module A) set out in Annex VI; ~~**or**~~

   (b) the EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; ~~**or**~~

   (c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI~~.~~ **; or**

   (d) where applicable, a European cybersecurity certification scheme as specified in Article 18(3) and (4) at any assurance level.

~~2. Where, in assessing the compliance of the critical product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer or the manufacturer's authorised representative has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to either any of the following procedures:~~

~~(a) the EU-type examination procedure (based on module B) provided for set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or~~

~~(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI. ; or~~

~~(c) where applicable, a European cybersecurity certification scheme as specified in~~

~~Article 18(3) and (4) at assurance level 'substantial' or 'high'.~~

3. Where the product is a critical product with digital elements ~~of class II~~ as set out in Annex III, the manufacturer **~~or the manufacturer's authorised representative~~** shall demonstrate conformity with the essential requirements set out in Annex I by using **~~one~~ any** of the following procedures:

(a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; **~~or~~**

(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI~~.~~**; or**

(c) where applicable, a European cybersecurity certification scheme as specified in Article 18 (3) and (4) at assurance level 'substantial' or 'high'.

Moreover, we propose to reduce the number of categories of products with digital elements listed in Annex III. Specifically, we believe the list could be limited to:

- General purpose boot managers;
- General purpose hypervisors;
- General purpose operating systems;
- General purpose microprocessors;
- Firewalls, intrusion detection systems and intrusion prevention systems;
- Antimalware/Antivirus

FRANCE

NOTE DES AUTORITÉS FRANÇAISES

Objet : Règlement du Parlement européen et du Conseil concernant les exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020.

Les autorités françaises prient la Présidence de bien vouloir trouver ci-après leurs propositions de commentaires sur les blocs 3 & 4.

Commentaires généraux sur les dispositions relatives aux produits critiques (annexe III et article 6)

Les autorités françaises rappellent que **le cadre du règlement sur la cyber-résilience (CRA) doit s'inscrire dans le respect des législations européennes antérieures**. Ainsi, les dispositions du CRA ne devraient pas avoir pour effet de nuire à l'effectivité de dispositifs qui le précèdent, à savoir notamment les dispositions du règlement sur la cybersécurité (CSA) créant les schémas européens de certification en matière de cybersécurité. En effet, les autorités françaises perçoivent, via les dispositions de la proposition de règlement, la mise en place de mécanismes d'évaluation obligatoire au titre du CRA, qui pourraient rendre l'utilisation des schémas de certification au titre du CSA caduque. Notamment, la mise en place d'un système graduel dans les types d'évaluation de la conformité en fonction de la criticité des produits avec un recours à l'évaluation par les tiers, introduit pour la France un **chevauchement des objectifs du CRA avec ceux du CSA.** En effet, comme rappelé dans les commentaires précédents des autorités françaises, le CRA doit établir un cadre d'obligations minimales pour autoriser la mise sur le marché des produits avec des éléments numériques. Contrairement à ce que le titre même du règlement laisse entendre, **les dispositions du CRA ne doivent pas adresser le niveau de résilience des produits**, mais bien mettre en place des conditions pour permettre à un produit d'être mis sur le marché de l'Union européenne. Dès lors, les méthodes d'évaluation de la conformité proposées par le CRA, et tirées du nouveau cadre juridique (NLF), ne doivent pas être interprétées comme attestant du niveau de robustesse d'un produit ou du niveau de cybersécurité d'un produit. Telle est l'interprétation des autorités françaises, sur la base de l'article 1 du CRA, qui dispose que le règlement « *établit les règles relatives à la mise sur le marché de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits (...)* ». Ainsi, pour les autorités françaises, le CRA doit poser des exigences élémentaires en matière de cybersécurité sans proposer une évaluation de la conformité plus exigeante pour certains produits. Une divergence d'analyse sur les objectifs du CRA telle que présentée représenterait un désaccord important.

Sur la nouvelle proposition d'articulation du CRA avec le CSA

Les nouvelles propositions de la Présidence sont à saluer en ce qu'elles introduisent les schémas de certification dans les méthodes possibles d'évaluation de la conformité au CRA. Toutefois, ce recours étant limité, conditionné, aux paragraphes 3 et 4 de l'article 18, la **nouvelle rédaction ne permet donc pas de répondre pleinement à l'objectif de préservation du recours aux schémas de certification au titre du CSA.** En conséquence, **les autorités françaises poursuivent leur réflexion sur ce sujet** pour trouver une solution qui puissent à la fois assurer une préservation des schémas de certification, tout en respectant le cadre NLF. Dès lors, au stade actuel de leurs réflexions, **les autorités françaises maintiennent donc une réserve d'examen sur cette partie du texte**

Concernant l'articulation du CRA avec la directive équipements radio (RED)

Les autorités françaises souhaitent de nouveau exprimer leurs inquiétudes concernant l'articulation des dispositions du CRA avec les travaux de standardisation actuellement menés dans le cadre du règlement délégué (UE) 2022/30 de la Commission du 29 octobre 2021 complétant la directive 2014/53/UE du Parlement européen et du Conseil en ce qui concerne l'application des exigences essentielles visées à l'article 3, paragraphe 3, points d), e) et f), de cette directive. En effet, les autorités françaises souhaiteraient que l'articulation entre les deux textes soient plus explicités, notamment dans le sens où les exigences au titre de la directive 2014/53/UE du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques (RED) seront d'application à partir d'août 2024 et que les dispositions du CRA sont applicables au plus tôt en 2026. Les autorités françaises souhaiteraient savoir si une fois appliqué, le CRA viendra complètement remplacer les exigences de la RED ou si certaines dispositions du règlement délégué seront maintenues, car elles ne sont pas couvertes par le CRA. On peut citer à ce titre le paragraphe 14 de l'acte 2022/30.Par ailleurs, l'article 9 qui articule le CRA avec le projet de règlement sur les Machines pose un problème important pour la prévention des machines. Il prévoit, concernant les produits soumis au CRA, que le fabricant qui applique le CRA remplit automatiquement les exigences du règlement Machines (annexe III, sections 1.1.9 et 1.2.1). Or l'ensemble des exigences de l'article 1.2.1 relatif à la fiabilité des systèmes de commandes des machines ne sont pas couvertes par le CRA. En outre, l'utilité de l'article 9 n'est pas démontrée, dans la mesure où l'article 8 du projet de règlement Machines prévoit déjà un principe d'articulation du règlement Machines avec les autres règlements, concernant des risques spécifiques mieux couverts par d'autres législations. Par conséquent les autorités françaises proposent la suppression de l'article 9 ou, à défaut, sa limitation à l'article 1.1.9. relatif à la protection contre la corruption.

Les autorités françaises se tiennent à la disposition de la Présidence pour toute precision utile.

LATVIA

Written comments from Latvia on "Block 4" of the Cyber Resilience Act

Article 41

3.Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated under Article 58 of Regulation (EU) 2019/881 and exchange information on a regular basis. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 11 of this Regulation, the designated market surveillance authorities shall cooperate with ENISA.

4.Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of other Union harmonisation legislation for other products, and exchange information on a regular basis.

5.Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing these authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 8 of this Article if such guidance and advice concerns the processing of personal data.

Authorities supervising Union data protection law shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks. They shall inform the designated market surveillance authorities of the Member State concerned of any such request.

[…]

9.The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law.

Proposal foresees informing and cooperation obligations for the market surveillance authorities with various other institutions (national cybersecurity certification authorities, ENISA, data protection authorities, competition authorities). We think that it is not clear in which cases the information must be provided. How the market surveillance authorities will evaluate what information is relevant for these other institutions?

9. ***Each Member State shall, as part of the overarching national market surveillance strategy according to Article 13 of Regulation (EU) 2019/1020, draw up an action plan outlining the market surveillance activities planned to ensure that appropriate checks are performed on an adequate scale in relation to this Regulation.*** ~~***The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities.***~~ *The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law.*

We are concerned about the administrative burden arising from annual reporting in paragraph 41.9. In accordance with the Market Surveillance Regulation 1020/2019 (Article 13), member states are obliged to develop national market surveillance strategies every four years. Section 5 of the strategy template foresees the provision of the information on the performed surveillance activities for all regulations/directives specified in the Annex of Regulation 1020/2019 (including Cyber resilience act). In order not to increase the administrative burden, we suggest harmonizing the reporting deadline with the regulation 1020/2019. The suggested wording is taken from current compromise text in the *proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC*.

Article 43

4.Where the manufacturer of a product with digital elements does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict that product being made available on its national market, to withdraw it from that market or to recall it.

That authority shall inform the Commission and the other Member States, without delay, of those measures.

It is not specified how the institution reports to the Commission and other Member States of the measures taken. Is it planned to use the ICSMS and Safety Gate systems that are already used under the Market Surveillance Regulation 1020/2019 and General Product Safety regulation?

Article 45

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***~~ ***informs*** *the relevant market surveillance authorities* ~~***to carry out an evaluation of compliance and follow the procedures referred to in Article 43.***~~

Latvia opposes the powers given to the Commission in this paragraph. Enforcement of the regulation and market surveillance activities are under the competencies of the Member States. National market surveillance authorities carry out market surveillance activities in accordance with the existing situation in their territories, identified risks and allocated resources. The Commission should not give the national authorities binding requests to perform market surveillance activities on specific products. The Commission can inform the national authorities about the existing risks and call for actions, but there should not be binding requests from the Commission to carry out market surveillance activities. The same comment is applicable to the article 46, paragraph 6.

Article 48

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.

The Commission or ENISA may propose joint activities; however, Latvia is of opinion that the participation in these activities should not be binding to the market surveillance authorities. Market surveillance authorities participate in joint activities on voluntary basis.

THE NETHERLANDS

Written comments by the Netherlands (NL) on the Cyber Resilience Act (CRA)

Concerns all 4 blocks

Horizontal Working Party on Cyber Issues (HWPCI)

17 March 2022

The Netherlands (NL) would like to thank the Swedish Presidency for the compromise text on blocks 1 and 2 of the Cyber Resilience Act (CRA) which we consider to be a big step in the right direction. We also thank the Presidency for the opportunity to provide written comments on blocks 3 and 4 again and the invitation to provide written comments on the rest of the CRA as well. We hereby would like to comment on the full text of the CRA, but do maintain a scrutiny reservation as there are still aspects of the proposal that we need further discussion on.

Recital 9: Scope and SaaS

We maintain our scrutiny reservation on the scope of the CRA. We welcome attempts to clarify the scope regarding Software-as-a-Service (SaaS). However even more clarity would be needed. We would welcome a workshop on this topic where we could discuss several examples of SaaS and how they relate to the definition of remote data processing solutions. An alternative would be to provide more examples in the recital.

New recital art 4 para 5

We fear that the wording of the compromise text is too narrow: this MS prerogative should not be limited to products that will be used for military, defence or national security purposes. MS should also be allowed to take measures safeguarding national security that relate to products with digital elements that are used for other purposes. An example would products used in private mobile networks (and therefore not specifically used for aforementioned purposes) that could pose national security threats. We refer to our comments regarding articles 2 and 4.

Recital 9a: remote data processing solutions

We support the proposed recital 9a, but we would expect it to directly follow recital 9 which also describes remote data processing solutions.

Recital 10: commercial activity / open source

We welcome most of the proposed changes in recital 10. The explanation that commercial activity relates to the definition of 'making available on the market' was necessary in our view, so we fully support the Presidency proposal on this point. We also welcome the broader scope of this recital, since the definition of making available on the market and the exclusion in it of products that are supplied outside the course of commercial activities is not limited to open source software. It is also relevant for other non-commercial examples. We also welcome the clear explanation that conditions regarding the development are not relevant when assessing whether a product is supplied in the course of commercial activities. We expect these changes to give some more clarity to open source developers.

However, we would like to propose alternative wording for the last 2 sentences of this recital because we think they can be confusing. The phrase starting with "taking into account of" seems to imply that the CRA only applies to Open Source that matches the definition and is offered on a commercial basis. Which is not the case, because the CRA also applies to all other commercial software. Something similar is the problem with the phrase that starts with "For the same considerations". No activity that charges a fee solely for the recovery of actual costs is considered a commercial activity. This is not limited to public administration activities.

We therefore suggest to amend the text as follows:

> (10) This Regulation applies only to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. The supply in the course of 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 when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise, by providing a software platform through which the manufacturer monetises other services, or by requiring as a condition for use, the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity. **Open-source software is understood as free software that is openly shared and freely accessible, usable, modifiable and redistributable, and which includes its source code and modified versions.** Taking account of the above-mentioned elements determining the commercial nature of an activity~~, only free and open-source software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable, supplied in the course of a commercial activity and therefore placed on the market should be covered by this Regulation.~~ **this Regulation should only apply to open-source software that is supplied in the course of a commercial activity.** ~~For the same considerations, p~~**P**roducts provided ~~by public administration entities~~ as part of the delivery of a ~~public~~ service for which a fee is charged solely to recover the actual costs directly related to the operation of that service**, as is often the case with products provided by public administration entities,** should not be considered on those grounds alone a commercial activity for the purposes of this Regulation.

Recital 11a

We support an additional recital on automatic updates. In our view, the requirement to provide products with automatic updates as the default setting however shouldn't apply to *all* products with digital elements as setting it as a default would cause problems in professional settings. The chance of disruptions to the continuity of organisations is high if an update is initiated outside the control of network administrators. This is not only the case in professional ICT networks, but especially true of industrial settings. We propose that the yet to be drafted recital clarifies that this requirement is not absolute, and is intended specifically for *consumer products.*

In addition, we suggest that the new recital 11a discusses the essential requirements in Annex I in general. It should for example explain that a product that would not be able to comply with a specific essential requirement without having to add a functionality to it, is in that case not required to add that functionality, as was explained by the Commission during the HWPCI meeting on 15 March.

We would also like to suggest mentioning in this recital that the requirements will need to be worked out in harmonized standards in which *state-of-the-art* technical measures to meet these requirements will be prescribed.

Recital 18a: due diligence

We welcome a recital on the due diligence obligation in article 10 para 4, and we support the risk based approach to this due diligence. In the case of a manufacturer integrating a component that is itself regulated under the CRA, it makes sense to suffice with the obligation to check if the component manufacturer is in conformity with the CRA, for example by checking the CE label. However, if the component to be integrated is not regulated, because it is not supplied in the course of a commercial activity (non-commercial open source for example), we want the recital give some more guidance on *how to determine the level of effort required* from integrators of non-commercially supplied components. When are efforts sufficient to fulfill the due diligence obligation?

A second suggestion for this recital is to mention the fact that the responsibility of the manufacturer integrating a component sourced from a third party does not stop after the due diligence during the integration, which typically would occur at the moment of placing on the market. He will also continue to be responsible for the effective vulnerability handling during the expected product lifetime.

Text suggestion regarding the responsibility for vulnerability handling to add to recital 18a:

> The responsibility of the manufacturer integrating a component sourced from a third party does not stop after the due diligence during the integration, which typically would occur at the moment of placing on the market. He will also continue to be responsible for the effective vulnerability handling during the expected product lifetime.

New recital 19a: actively exploited vulnerabilities

We welcome a workshop (and a recital) on actively exploited vulnerabilities as proposed by the Presidency. We find it very important to have further discussions on the notification obligations and their implications, such as the identification of an exploited vulnerability, the handling of notifications for which no patches are available yet, and the forwarding of notifications.

Recital 22 en 22a: substantial modification and security updates

We welcome the clarifications. However, we still need to scrutinize the text of these recitals.

Recitals 34 and 35: reporting obligations

These recitals will need to be amended based on the proposed changes for article 11 on reporting obligations.

Article 2 and 4 regarding national measures versus maximum harmonisation

As was discussed during last meeting of the HWPCI, an important principle to be held in mind is that the CRA only regulates *the making available of* products and does not regulate the *use* of products. As long as a national measure does not limit the free movement of products that comply with the CRA on the internal market the national measure would not conflict with the maximum harmonisation of the CRA. MS should therefore be allowed to require higher CS requirements for products to be used in certain situations, for example in national regulation aimed at the security of mobile networks or other NIS entities, or in public procurement procedures. Another national measure that should not conflict with the maximum harmonisation in the CRA would be to ban specific products based on non-technical reasons, not only because national security is a MS prerogative, but also because this is not covered by the CRA and therefore no maximum harmonisation regarding non-technical measures exists. We will look for text suggestions to make this clear in articles 2, 4 and corresponding recitals together with some other MS that share these concerns.

Article 6 – Critical and highly critical products with digital elements

We support maintaining a provision that requires third party assessment of critical products. It is important that it is clear which criteria are used to make the list of critical products in Annex III. We therefore support moving these criteria from para 2 to para 1 as included in the compromise text dated 10 February. We support keeping the list in Annex III because this provides the legal certainty that manufacturers need, and will avoid unnecessary discussions with national market surveillance authorities.

Article 10 – Obligations of manufacturers

In the meeting of the HWPCI on 15 March it was clarified by the Commission that the manufacturer is in fact intended to be responsible for the vulnerability handling in case a vulnerability is identified in an integrated component sourced from a third party. We think this is not yet clear in the proposal, as we understood that the CRA only addresses the responsibility of the integrator in 2 instances:

- article 10 (4) prescribes exercising due diligence when integrating of components in order to comply with the prescription in article 10 (1) to ensure that the product with digital elements has been designed, developed and produced in accordance with the essential requirements,
- and article 11 (7) prescribes the reporting of an identified vulnerability in a component to the person or entity maintaining the component.

As suggested before, we would like to clarify that the manufacturer is imposed with more responsibilities regarding the component he chooses to integrate in his product. If a full responsibility to ensure that the product including all of its components (also the ones sourced from third parties) has been designed, developed and produced in accordance with the essential requirements (article 10 para 1) would not be proportionate, the manufacturer should at least be responsible for the effective vulnerability handling in article 10 para 6. This means that a manufacturer cannot suffice with the reporting of an identified component to the person or entity maintaining a not-regulated component: he should also make sure the vulnerability is handled effectively (either by himself or the person or entity maintaining the component).

Our previous text proposal to add this notion in article 10, para 6, was unintentionally limited to not-regulated components. We would therefore like to correct our previous text proposal:

> 6. Manufacturers shall ensure, when placing a product with digital elements on the market and for the expected product lifetime, that vulnerabilities of that product ***including all of its components,*** are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.

In response to the issue raised by the Commission in the last HWPCI we are currently reflecting on a solution for specific situations in which the requirement to handle vulnerabilities for the duration of the entire expected product lifetime becomes disproportionate, for example when the product would in theory have an indefinite product lifetime, or when the product is used by a very small number of users which would make vulnerability handling unrealistically burdensome. This could be described in the corresponding recital, for which we will provide a text proposal at a later stage.

Article 11 – reporting obligations of manufacturers

We support the modifications in most paragraphs of article 11, however the proposed reporting structure in para 1 and 2 of the compromise text leaves too much room for interpretation. It remains unclear which Member State's CSIRT(s) first receive(s) a notification from a manufacturer and what is meant with "Member States concerned":

- Is it the CSIRT of a single Member State? If yes, we find it important that it is specified in the legal text which jurisdiction will be used for determining which Member State (and its CSIRT) would be designated per manufacturer (f.e. HQ, main establishment principle, designated representative, etc.). This is especially important with regard to non-EU manufacturers.
- Or, do the CSIRTs from all Member States in which the product is made available, all receive a notification from the same manufacturer? If yes, the Netherlands would not be in favour of separate notifications in multiple Member States, instead we would prefer the use of automated processes in the single reporting platform.

If the correct interpretation of the compromise text would be that a notification is first received by a single Member State's CSIRT, we find it important that this notification will be forwarded as soon as possible to all other CSIRTs of Member States in which the product is made available. We think this is insufficiently reflected in the current compromise text in which the CSIRTs should forward the notification – without undue delay – only to ENISA, not to other CSIRTs.

A text suggestion for paragraph 1 could be:

The **designated** CSIRTs ~~s~~ shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to **all other designated CSIRTs of Member States concerned [where the product is made available?] and** ENISA (…)

Regarding paragraph 2b a suggestion could be to integrate this in the reporting platform.

Annex I – Essential cybersecurity requirements

Regarding part 1 sub 3 a: We support adding the text regarding automatic updates by default, however it is necessary to limit this requirement to consumer products. For non-consumer products, a voluntary opt-in for automatic updates could be an alternative to an opt-out of automatic updates. If this is not carved out in the essential requirement itself, it would be necessary to explain this in the corresponding recital 11a. We refer to our comments regarding recital 11a.

A smaller issue: the referral to Annex II 8a seems incorrect, and we don't understand "according to requirement in Annex II 8a", because this does not seem related to the type of technical security support offered by the manufacturer.

Annex II – Information and instructions to the user

Regarding sub 9a: We should not include 'expected' here. This refers to the secure use of a product, so these instructions should not be limited to the support period in article 10 para 6, which uses the term 'expected' product lifetime.

Regarding sub 9e: We would like to insert 'where applicable'.

Regarding sub xx: we do not see sufficient reason to prescribe the way in which the SBOM should be provided to users, considering that the inclusion of an SBOM is a voluntary decision of the manufacturer.

Annexes I and II

A general remark regarding the Annexes: it would be good to check on consistency of the wording of (for example) information obligations that are described in both an article and in the Annexes.

Annex III – list of critical and highly critical products

The proposed rearrangement of the list in Annex III is an improvement to clarify what criteria were considered in the decision to place a certain product in Annex III as either critical or highly critical.

We maintain a scrutiny reservation regarding the contents of the list.

Article 38 – Information obligation on notified bodies

Article 38 prescribes notified bodies to inform the notifying authority of (among other things) any suspension or withdrawal of a certificate. We think this information would be especially relevant for market surveillance authorities.

We propose to include an information obligation to also inform *market surveillance authorities* by adding a paragraph 3 to article 38:

> **3. Notified bodies shall inform the market surveillance authorities of any refusal, restriction, suspension or withdrawal of a certificate.**

Article 45 – Procedure at EU level regarding products presenting significant CS risk

We maintain a scrutiny reservation on the proposed competence for the Commission. It is important that the Member State maintains its responsibility for its market surveillance, whilst keeping in mind the importance of cooperation between Member States. We want to stress the importance of the independent role of market surveillance authorities.

We therefore propose to at least add more safeguards to better reflect that this would be a 'last resort' measure. Examples could be to prescribe in para 2 that the Commission procedure should start with a consultation of the national market authorities asking them for their reasons not to take measures and allowing national market authorities to act themselves within a specific timeframe. Another example of additional safeguards could be to introduce an objection procedure similar to the objection procedure for national market surveillance authorities in Article 44.

Article 57 – Entry into force and application

Without a suitable standard for its product with digital elements, it will be practically impossible for a manufacturer to use self-assessment. Conformity assessment bodies would be inundated with assessment requests, not only for critical products but also for all products with digital elements for which there is no suitable standard available yet.

Considering the wide variety of products with digital elements that will be in scope of the CRA it will not be possible to draft one standard that would fit all of them, so we will need to finish various standardisation procedures before the date of application**.** We should consider that the group of experts working on the drafting of one standard will largely overlap with the group of experts needed to draft the other standards under the CRA, so it is difficult to simultaneously work on different standards. Moreover, as we understand, there are no standards for cybersecurity of software yet and this novelty could proof to be particularly challenging.

For the CRA to become a success it is crucial that a realistic timeframe is provided, taking into account not only the drafting time but also the procedure of Commission approval and the implementation by manufacturers of harmonized standards once they are available.

Also considering that the mapping results of suitable cybersecurity standards and gaps will only become available this summer, it is important at this stage to not be too optimistic in expecting 24 months to be sufficient.

We will need to look at the standards that are currently being worked on for the Radio Equipment Directive to learn from it in setting a realistic transition period, and we would like to hear from CEN/CENELEC from their experiences and what timeframe they would consider realistic. All while keeping pressure on the standardisation organisations and the experts working on the drafting to avoid unnecessary stalling.

FINLAND

FI written comments on CRA Blocks 3-4

Finland would like to give the following comments on CRA Blocks 3-4:

Article 6

We support the clarification of highly critical products to the headline. We see the cumulative criteria in para 1 a good progress to clarify the logic in Annex III products. However the word "criteria" seems to be used in this context in a misleading manner since Art. 6(1) subparagraph 2 a "the cybersecurity-related functionality" cannot be seen as a criteria as such. Criteria by definition is something that can be unambiguously stated wheter it fulfills or not. This is not the case in the referred paragraph.

Either, instead of referring to "criteria" the word could be changed to "aspects" or the paragraph should be rephrased as statement:

"a) the product with digital element or its cybersecurity-related function performs critical functionality to security, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection;"

Also, we don't see criteria relevant in para (1) since the list in Annex III has already been formulated and there is no need to reason the foundations how the list in Annex III is created. We would like to see the criteria moved to para (2) where we see it more relevant to define on what basis list in Annex III could be changed by delegated act.

Reflecting the discussion from the meeting about deleting art. 6 and annex III, given our national experiences from cybersecurity label we strongly support the mandatory third party assessment for most critical products. However, we are open for the discussions on how critical products are defined in the proposal.

We still are cautious about delegated power proposed in Art. 6(2). Repeating our previous comment we acknowledge potential need to update Annex III list in the future, we feel that the proposed delegated power as such would allow to create wide new obligations. Delegated acts can only add or delete non essential elements of the legislative act and from our point of view this delegated power that creates obligations from self assessment to third party assessment could potentially have impact on the key elements of the proposal. Amending list in Annex III would have major impact on manufacturers' costs of compliance with the proposal.

Delegated powers in art. 6 and elsewhere should be assessed carefully so that they are proportionate and defined in a manner that is required for a delegated act. We still leave a scrutiny reservation on this issue.

We support the clarification in para 5 about the assurance level of certification. However it still remains unclear what exactly can be highly critical product compared to the list in Annex III.

Article 9

We see that compromise proposal is improvement to COM proposal with addition of "requirements related to cybersecurity". However this article is still too open. As different interpretations can be argued for which requirements are related to cybersecurity and which are not, this article does not have much added value for interplay between CRA and the Machinery Regulation. Instead article 9 could increase legal uncertainty if it's complience is not defined more precisely. With further definitions we see also removal of article 9 as feasible option in order avoid legal uncertainty.

CRA and the Machinery Regulation focus on different aspects. CRA focuses on "cybersecurity" and thereby the aim is to increase the resilience of digital products. The Machinery Regulation lays down "health and safety" requirement for the design and construction of machinery and thereby the requirements regarding the protection against corruption just ensures that the machinery will e.g. always stays "safe" so that nobody will be in danger due to malware (some are calling this "cyber-safety requirements"). But the requirements of the Machinery Regulation are not regarding the resilience, but more of the health and safety features of the Machine. Even if some requirements of the CRA and the Machinery Regulation would address the same aspect or different views of the same aspect, the manufacturer of the machinery will find out very easily, if there would be a duplication of requirements during the risk assessment. In this case we see that there would be no additional work or costs for the manufacturer. Thus, Article 9 of the CRA should be further clarified with references to exact points or subsections within sections 1.1.9 and 1.2.1 or removed, because without this, the Article 9 would provide no added value, but only confusion. We see that most of the section 1.2.1 on Machinery Regulation are not covered by CRA.

Article 18

We would like to propose a slight simplification to the text in Art. 18(1):

" Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements ~~covered by those standards or parts thereof,~~ set out in Annex I, **or parts thereof**."

Article 19

We support changing the proposed article 19 according to Machinery Regulation.

Article 24

We do not support the new wording in Art. 24(5) about SMEs. We see this as an issue of equal treatment and the practical application of this is very unclear (what is SME, are all specific interests of SMEs similar wth each other, what does taking into account mean, what are other relevant indicators?). We do see that taking SMEs into account is important but in an way that does not conflict the equal treatment. We would suggest putting this part to recital and other than that rely on art. 37(2) as a general leading principle on this matter.

Article 29

Paragraph 4

We would again suggest adding importers and distributors to the list where the involvement is not allowed in order to avoid conflicts of interest. We see importers and distributors equally relevant compaired for example to suppliers or marketing. This is also similar with the Machinery regulation.

4. A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, **importer, distributor,** installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those arties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.

A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, **import, distribution,** development, production, the marketing, installation, use or maintenance of those products, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services.

New Article X

We support the new article on appeal against decision of notified bodies as such.

Chapter V

We would especially find it important that overlapping with art. 16 of Market Surveillance Act is limited to only what is necessary. We provided the information on overlpping parts of the regulations in our previous comments on Block 4.

Article 44

Current article leaves room for specification what happens if the decision is not delivered within given time frame – will the objections expire if Commission does not deliver positive or negative decision within nine months.

Article 53

We support the new, more detailed phrasing of para (4) and find detailed phrasing essential in order to create legal certainty.We refer to Council Legal services argument that legal requirement for sanctions is to be spesific and proportionate.

We support including obligations set out in Articles 12 – 17; 20; 22(1)-(4); 24(1)-(3); and 42. Regarding obligations set out in Articles 29, 31, 37 and 38 proportionality of sanctions should be further assessed and necessity of these sanctions could be questioned. Sanctions should only be used as final mean if no other means are available. We see that as authorities would have several other ways than sanctions to interfere with non-compliance of notified bodies, these sanctions might not be necessities.

Regarding paragraph 5, we point out that supplying incorrect or misleading information that has legal effects to authorities is criminal offence in Finland under section 16 of the Finnish Criminal Code.

Council of the European Union
General Secretariat

Interinstitutional files:
2022/0272 (COD)

Brussels, 21 March 2023

WK 3918/2023 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	General Secretariat of the Council Delegations
N° Cion doc.:	ST 12429 2022 + ADD 1-6
Subject:	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: Delegations' comments on Blocks 3 & 4

Delegations will find attached comments by the BE, DK, DE, IT, FR, LV, NL and FI delegations on the above-mentioned legislative proposal.

The IT and NL comments also apply to Blocks 1 and 2.