Council of the European Union
General Secretariat

Interinstitutional files:
2026/0011 (COD)

Brussels, 02 July 2026

WK 5879/2026 INIT

LIMITE

CYBER

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (18.08.2026)

PUBLIC

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:	General Secretariat of the Council
To:	Horizontal Working Party on Cyber Issues
N° Cion doc.:	5611/2026 + ADD 1-4
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) - Member States' consolidated comments on Articles 98-122

Delegations will find attached consolidated comments received from Member States on Articles 98-122 of the above-mentioned proposal.

CSA2 Art. 98-122 Deadline: ***19 June 2026***

From: AT, BE, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, IT, LT, LV, NL, PL, PT, RO, SE, SK **Updated: 01/07/2026 10:43**

PUBLIC

Guidelines to be followed

Please kindly provide your contributions in the table below.

Drafting suggestions: you may use '**track changes**'* or formatting (for example **bold-underline** for additions and ~~strike-through~~ for deletions, **where necessary, in a different colour**). *Track changes can only be connected once the cursor is placed in editable areas (Drafting or Comments columns).

To make it feasible to consolidate all contributions, the structure of the table must not be changed, so **no rows can be added or deleted.**

New provisions may only be added in any of the **'existing cells'.**

Name of document: please add the **two initials** of your delegation's country followed by a space (to the MS Word document name), followed by any optional text, for example, for Austria: **AT comments on … .docx**

Thank you for your cooperation!

Commission proposal	Drafting suggestions and Comments
General Comments	AT (Comments): Firstly, it should be noted that AT supports the creation of a uniform framework for improved security in the ICT supply chain and the underlying objective of further strengthening cyber resilience in principle. It is important to adapt the security landscape to the everchanging challenges of the global cyber domain. The current proposal is a solid first step in this directin and provides a sound foundation on which to further build on. However, there is still plenty of room for further improvements. The proposed measures must be considerably more nuanced if they are to withstand the test of practical implementation. Greater transparency and objectivity are required in order to establish a rock-solid framework, grounded in the principles of the rule of law. Additionally, the risk-based approach inherent in the EU cybersecurity acquis must continue to be upheld.

Commission proposal	Drafting suggestions and Comments
	The proposed Title on the security of ICT supply chains does not yet fully comply with the outlined prerequisites in AT's view. [redacted] Therefore, AT proposes the comments laid down in this document to work towards a more balanced, transparent and robust approach of safeguarding the ICT supply chain. [redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] PUBLIC CZ (Comments): CZ: We believe that the supply chain security mechanism is one of the key parts of the new cyber package that needs proper understanding of the procedures and thorough assessment of its impacts. For this reason, we have a **scrutiny reservation to the whole title** and are looking forward to to further thematic discussions at the Council under the IE Presidency. As we believe it is necessary to discuss the approach before redrafting the text, **please see the Czech general comments on a possible direction of work, shared separatedly from this document**, that sumarize the main points and pilars to be reflected in this title. This being said, please find below a few concrete drafting suggestions that are in any case not exhaustive and that will be finetuned and complemented as the negotiations will proceed. DK (Comments): DK: Overall we are positive about having a framework at European level to address non-technical risks. We considers this is best achieved through a risk-based and proportionate framework focusing on the most critical supply chains and avoiding unnecessary administrative burden. Given the complexity and potential impact of the Trusted ICT Supply Chain Framework, it is essential to ensure clarity and coherence in the terminology and structure. We suggest making clearer groupings of articles according to

Commission proposal	Drafting suggestions and Comments
	their purpose and distinctions between the different measures and the more procedural elements, such as methods of identification and designation. The alternative structure could be as follows, grouping articles in the title into five clear groups: 1. Scope; 2. Identification (e.g. of countries, ICT-assets etc); 3. Mitigating measures; 4. Procedural requirements; 5. Governance, supervision and enforcement. **1. Scope** This section would include an overview of the framework and the security mechanism (art. 98 & 101) with the following elements: • identification (art. 99, 102, art. 103 (7 & 6) & 104)); • mitigating measures & exemption (art. 100 (4), 103 (1), 103 (7), 110 (1), 111 (1), 103 (2) 6 art. 105); • procedural requirements (art. 106, 107, 108 & 109); • governance, supervision and enforcement (art 112 – 117). **2. Identification measures** This section would include: • Identification of the relevant risks (art. 99) – risk assessments (incl. Roles and responsibilities). • Identification of key ICT assets (art. 102). • We suggest including criteria for identifying critical supply chains as well as references to definitions in art. 2 (33), (34), (35) (40). • Regarding designation of countries and entities: • We suggest clarifying and explicitly stating the connection between designation of a 3rd country (art. 100 (1 & 2) and the identification of a high-risk supplier (art. 104 (2)). There should be a clear reference to

Commission proposal	Drafting suggestions and Comments
	definitions relevant for identification of a high-risk supplier in art. 2 (37), (38), (39) (41) (42) & (43). • Finally, this section should address both designation of an entity as a high-risk supplier by way of designated country and by way direct designation (art 103 (7 & 6)) **3. Mitigation measures** This section would include: • Exclusion measures (art. 100 (4)) • Prohibition measures (art. 103 (1) & (7), 111 (1) & reference to art. 104 (1)) • Phasing out measures (110 (1)) • Other mitigating measures (103 (2) (9)) • Assessment of potential risks and dependencies (art. 103 (4)). • Exemptions from certain measures (105 (1)) • Covered NIS 2 entities & EU entities (art. 103 (8-10)) **4. Procedural requirements** This section would include: • Rights of defence (art. 106) • Register (art. 107) • Confidentiality (art. 108) • Fees (art. 109) **5. Governance, supervision and enforcement**. This section would include: • Competent authorities (art. 112). • We suggest including or referring to the obligations under art. 104 (6 & 8) as well as clarifying the role of the relevant authorities mentioned in art 100 (4) last paragraph • Network for cooperation and support services of the Commission (art. 113).

Commission proposal	Drafting suggestions and Comments
	• Supervisory and enforcement measures (art. 114). • We suggest that the enforcement measure under art 100 (5) (withdrawal of a European cybersecurity certificate) be moved to this section. • Penalties (art. 115) • Mutual assistance (art. 116) • Jurisdiction and territoriality (art. 117) Regarding the structure: Given the complexity of the proposed revised structure, we have not included detailed drafting suggestions for the individual articles at this stage - doing so would be premature. We would, however, welcome comments and discussion on the proposed revised structure to help guide the next steps of negotiations in Council. EE (Comments): We support establishing a separate expert group for risk assessments conducted under CSA2. This would help clearly distinguish them from non-mandatory technical assessments and allow for the involvement of experts with the specific expertise these assessments may require. ES (Comments): **ES — (Comments):** **TITLE IV — GENERAL POSITION OF SPAIN** Spain supports the establishment of a formal Union-level mechanism for the security of ICT supply chains and does not seek to weaken Title IV. Spain's objective is to ensure that a cybersecurity instrument does not become, without adequate safeguards, a transversal mechanism for the exclusion of third countries, suppliers and ICT assets on grounds that are not substantiated by objective, cybersecurity-specific evidence. [redacted]

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] *The texts requested for incorporation into the recitals and into Articles 1 and 2 appear in the "Drafting suggestions" column of this and the following rows. Spain's drafting proposals to the operative articles of Title IV follow in the corresponding rows.*

PUBLIC

Commission proposal	Drafting suggestions and Comments
	FI (Comments): We welcome the goal of the proposal to strengthen the security and resilience of ICT supply chains within the EU to ensure the functioning of the internal market. While we welcome the overall goal of the proposal, the proposed measures should be proportionate, risk-based and predictable. The risk assessment framework should be clear and member states should be involved clearly throughout the process. Ensuring proportionality is essential for Finland to ensure that the measures do not exceed what is necessary in terms of possible de facto restrictions to fundamental rights. As the proposal already recalls, it is important that Member States retain the possibility to introduce further national measures that are in line with union law, especially to safeguard the security of communications networks. Furthermore, while we welcome the goal of the proposal, it is important that competences between the EU and member states remain clear in terms of national security and defence. Our written comments reflect these views based on our official position with the aim of strengthening the overall quality, clarity and coherence of the proposal. HR (Comments): The proposal represents an important and timely step toward strengthening the security and resilience of the Union's ICT supply chains. In light of the growing sophistication of cyber threats and the increasing strategic importance of digital infrastructure, establishing a common framework for assessing

Commission proposal	Drafting suggestions and Comments
	cybersecurity risks is both justified and necessary. Greater scrutiny of vendors and supply chain dependencies can significantly contribute to the protection of critical infrastructure, public administration, and essential services across the EU. The effort to introduce harmonized risk-management measures at Union level is therefore welcome and reflects the evolving cybersecurity landscape. At the same time, given the potentially far-reaching legal and economic consequences of such measures, it is important that the relevant criteria and designation mechanisms are formulated with sufficient clarity, objectivity, and legal certainty. [redacted] HU (Comments): - We are deeply concerned as we believe the proposal, in its current form, contains several questionable elements that could be challenged on pragmatic grounds. [redacted] [redacted] This is why we suggest that this issue should be approached with great caution and in a very vigilant manner. [redacted]

Commission proposal	Drafting suggestions and Comments
	[redacted] - The relationship of ICT supply chain requirements with DORA should clearly be declared. IT (Comments): Italy welcomes the ambition of the proposed framework on ICT security, which aims to provide a structural response to systemic challenges. In this regard, the overall approach merits support. At the same time, we would like to emphasise the need for the following improvements: [redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	NL (Comments): The Netherlands would like to thank the Commission for its proposal to mitigate cyber risks at EU level. The revision of the Cybersecurity Act, more

PUBLIC

Commission proposal	Drafting suggestions and Comments
	specifically the introduction of a new European framework for securing ICT supply chains, directly affects cybersecurity, strategic dependencies and the functioning of the internal market. The risk-based approach, underpinned by thorough risk analyses is a strong foundation to enhance the resilience to the EU. We would therefore like to underline our support for this framework, as it is in our view the most pragmatic and coherent way to face the threats that affect the Union, and to manage the risks emanating from those threats. We would therefore like to offer a number of considerations to further strengthen the effectiveness and practical implementation of the framework. [redacted]

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] PUBLIC Overall, we support a framework that is risk-based, proportionate, focused, predictable and complementary to national measures. Strengthening the resilience of European ICT supply chains should go hand in hand with safeguarding competitiveness, investing in EU alternatives and innovation and the proper functioning of the internal market. PL (Comments): Poland stresses that any adopted mechanism should be led by the Member States, clear and proportionate. Currently, there are too many ways to initiate the procedure, as well as measures being introduced seemingly without a risk-based approach. I [redacted] SK (Comments): The Slovak Republic would like to make a general comment on Title IV. The Slovak Republic supports the principle of identifying high-risk suppliers as part of assessing the security of the ICT supply chain. However, we are of

Commission proposal	Drafting suggestions and Comments
	the view that the proposed mechanism set out in Title IV of the CSA2 proposal requires substantial revision in order to ensure its proportionality and better alignment with the existing EU acquis as well as the Union's international obligations. The objective should not be the disproportionate centralisation of decision-making powers at Union level.
	[redacted]

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] PUBLIC
	DE (Comments): **Germany maintains a scrutiny reservation with regard to Chapter IV 'SECURITY OF ICT SUPPLY CHAINS' of the CSA 2 proposal. The internal assessment of the proposal's overall policy direction is still ongoing, and, in light of the issue's considerable political significance, it is premature to provide detailed comments and proposals for change of the text at this stage.** **Nevertheless, we would like to emphasize some general considerations (Subject to change or addition)** • Germany shares the general objective pursued with the proposals in Chapter IV to measurably increase the level of cybersecurity in the EU and make risks along the supply chain addressable. • Germany sees a need for action regarding EU-wide access restrictions for so-called "high-risk suppliers" to critical infrastructures both at the national and European level. Specifically,

Commission proposal	Drafting suggestions and Comments
	with regard to a potentially uniform definition of critical components. • The regulations proposed in Chapter IV are in some cases very far-reaching and the timeframes for their implementation - in particular the mandatory phase-out of the affected ICT components within 36 months - are very ambitious. • In the process of assessing its position on specific regulations of Chapter IV of the Cyber Security Act 2, , Germany takes, above all, into account security policy considerations and the overall societal costs of a security incident. • Furthermore, Germany takes other aspects into account, particularly the potential impact on the innovation capability of European companies, diversification and costs, existing sectoral legislation on security in the IT supply chain as well as supply security – also as a location factor for the economy and industry – also with regard to public administrations, insofar as they themselves operate affected infrastructures or use corresponding components. [redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] PUBLIC ES (Drafting suggestions): **ES — (Drafting suggestions):** [redacted]

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] PUBLIC FI (Comments): **Also, on the relation of implementing acts to the primary act: it should be clarified in recitals and articles that the implementing acts suggested throughout the CSA2 truly *implement* the obligations laid down in this primary act and do not modify or supplement it as regards the substantive content of it. This distinction is important to clarify in the text in light of Article 291 TFEU and the case law of the Court of Justice, according to which implementing acts are technical in nature and are limited to ensuring uniform conditions for implementation and may not amend or supplement the essential elements of the primary act. This in turn is important to demonstrate proportionality.**
	ES (Drafting suggestions): **ES — (Drafting suggestions):**

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

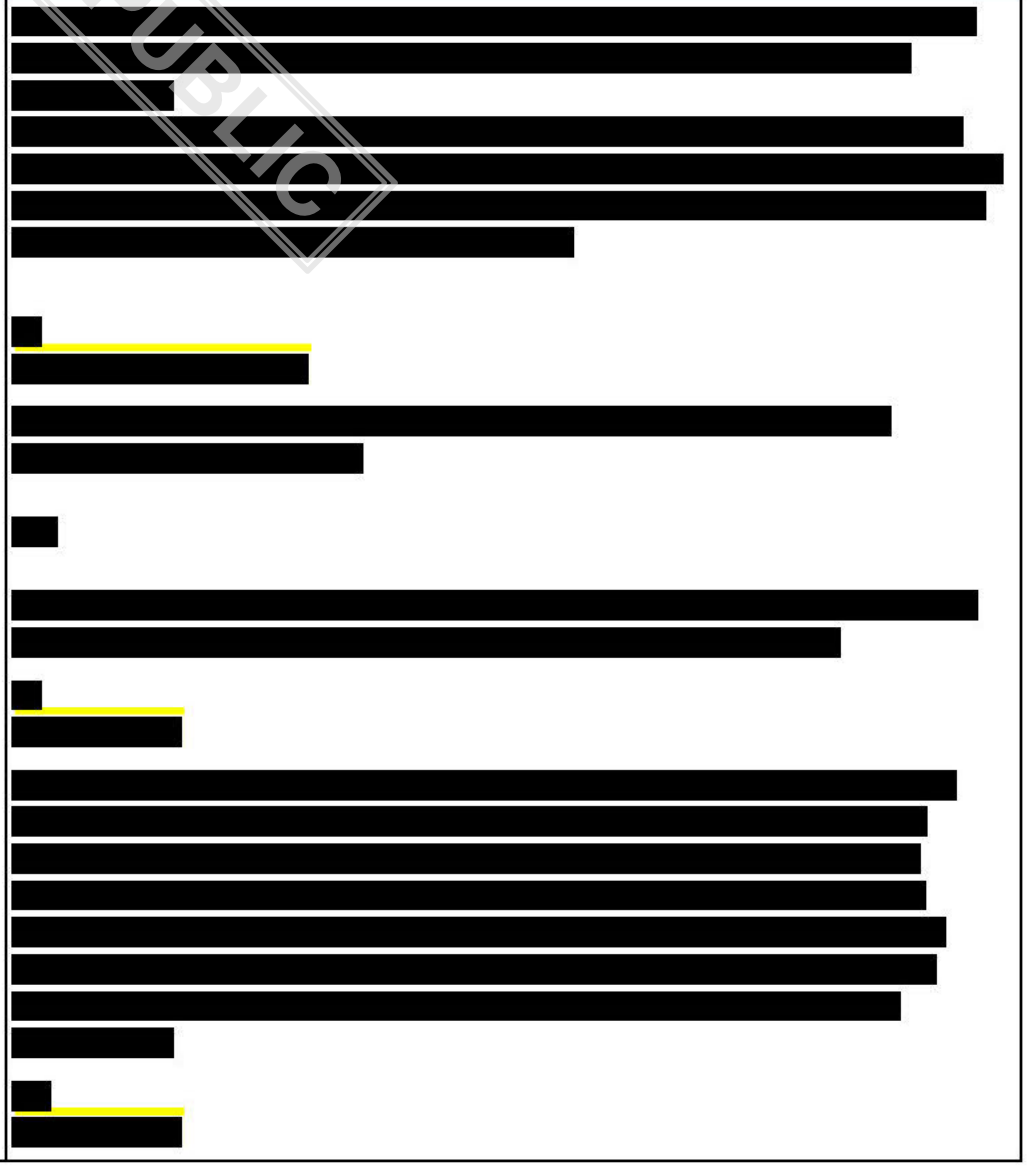
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] PUBLIC FI (Comments): Corresponding definitions of the ICT supply chain title in Article 2 should be clarified accordingly. For example, definitions on ICT product/services/process in art. 2 (16)-(18) and on ICT components in art. 2 (33) are too broad. Furthermore, art. 2 (34) on ICT assets is currently formulated with "software or hardware" – should be "software *and* hardware". **Necessary amendments for definitions relating to title IV could be checked with ICT experts with legal terminology knowledge/council legal services.**
TITLE IV **SECURITY OF ICT SUPPLY CHAINS**	DK (Comments): DK: The following comments and drafting suggestions are made within the existing structure of title IV. We propose the following material changes: 1. Making the distinction between security risk assessments conducted in accordance with article 22 of NIS 2 directive and the present regulation clear; 2. Strengthening involvement of Member States in both the identification of third countries posing cybersecurity concerns, the identification of high-risk suppliers and in the assessment of potential risks and dependencies

Commission proposal	Drafting suggestions and Comments
	when deciding mitigating measures. One way forward to be establishing a dedicated group or structure with a mandate to conduct security risk assessments in accordance with this regulation. We would welcome a thematic discussion on ways forward in HWPCI to guide the negotiations. 3. Empowering the Commission to lay down technical and methodological requirements for assessing the exclusion of high-risk suppliers from the listed activities under article 100(4) in close consultation with Member States; 4. Defining criteria for identifying "critical supply chains" to ensure an appropriate and proportional scope for setting mitigating measures. FI (Drafting suggestions): "Security of ICT supply chains of entities within the scope of Directive (EU) 2022/2555"
CHAPTER I ***Trusted ICT supply chain framework***	[redacted]

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 98 *Scope of the framework*	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
1. The trusted ICT supply chain framework shall provide for a security mechanism at Union level to address non-technical risks in sectors of high criticality and other critical sectors as referred to in Directive (EU) 2022/2555. The mechanism shall identify key ICT assets in critical ICT supply chains and set out appropriate and proportionate mitigation measures on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] ures

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

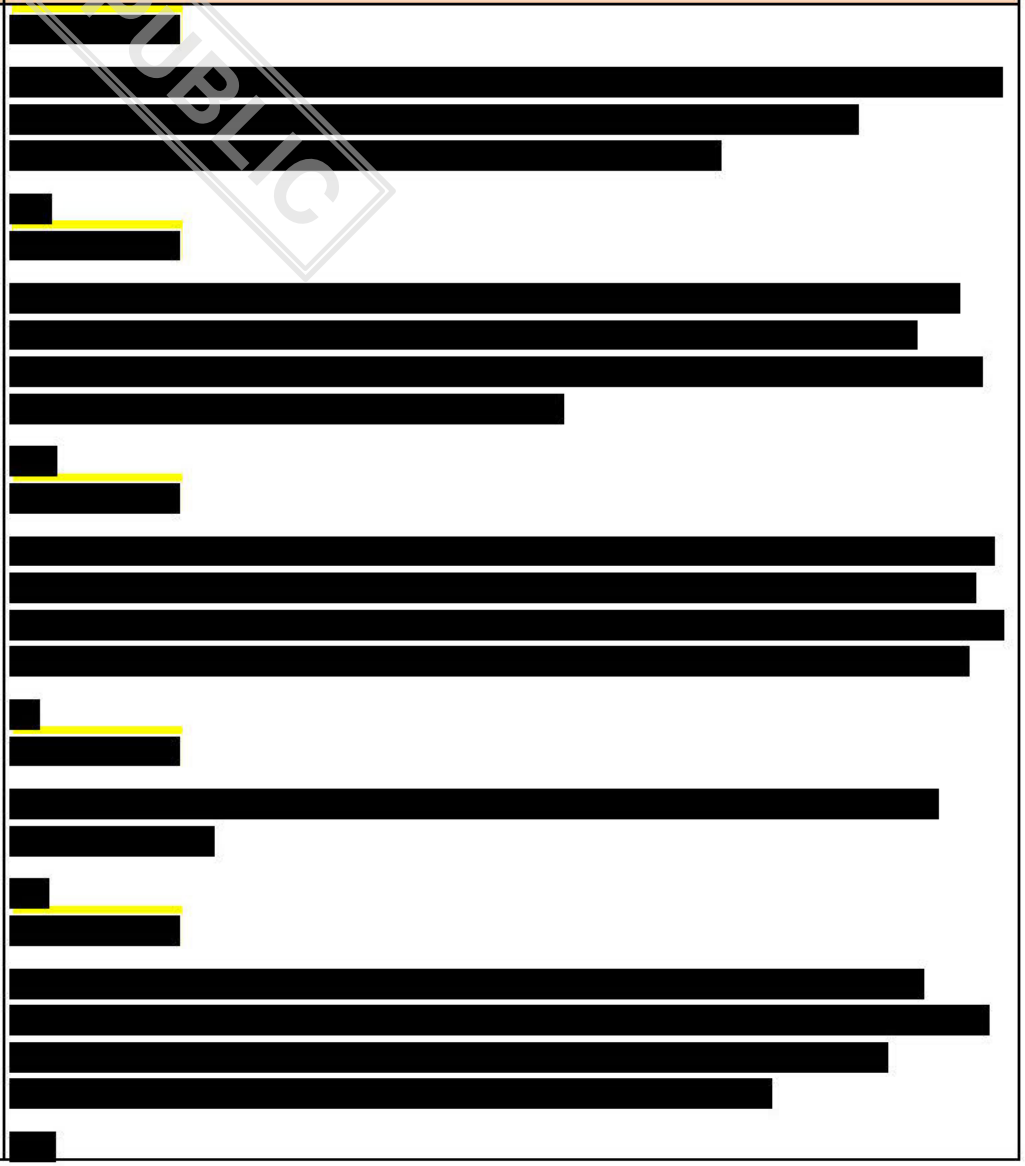
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]
2. The obligations set out in this Title shall be without prejudice to obligations set out in Article 13 of Regulation (EU) 2024/2847 and in national provisions transposing Article 21 of Directive (EU) 2022/2555.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
3. The provisions laid down in this Chapter shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity in ICT supply chains, provided that such provisions are consistent with their obligations under in Union law.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

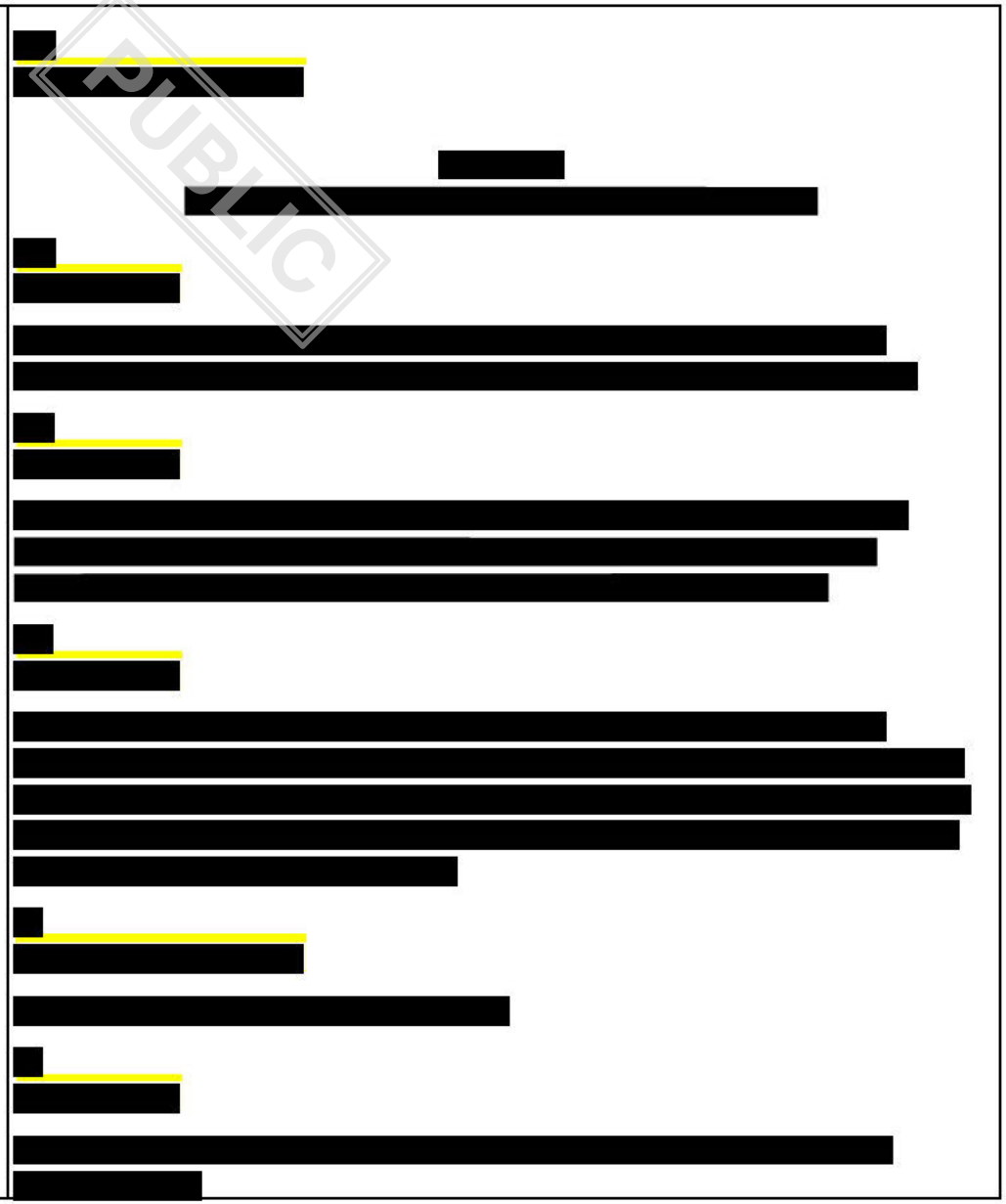
Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 99
Security risk assessments



Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. The Commission or a group of at least three Member States may request the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 ('NIS Cooperation Group') to conduct the Union-level coordinated security risk assessments in accordance with Article 22 of that Directive. Where a security risk assessment is conducted following such request, it shall include in particular the proposed identification of the key ICT assets of the respective ICT supply chain as well as the main threat actors, risks and vulnerabilities affecting those assets. The Union-level coordinated security risk assessments shall develop risk scenarios and propose measures to mitigate the identified risks.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. The Union-level coordinated security risk assessments shall be completed within six months from the request referred to in paragraph 1. Upon request of the Commission, the NIS Cooperation Group may agree to a shorter period.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted] LT

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

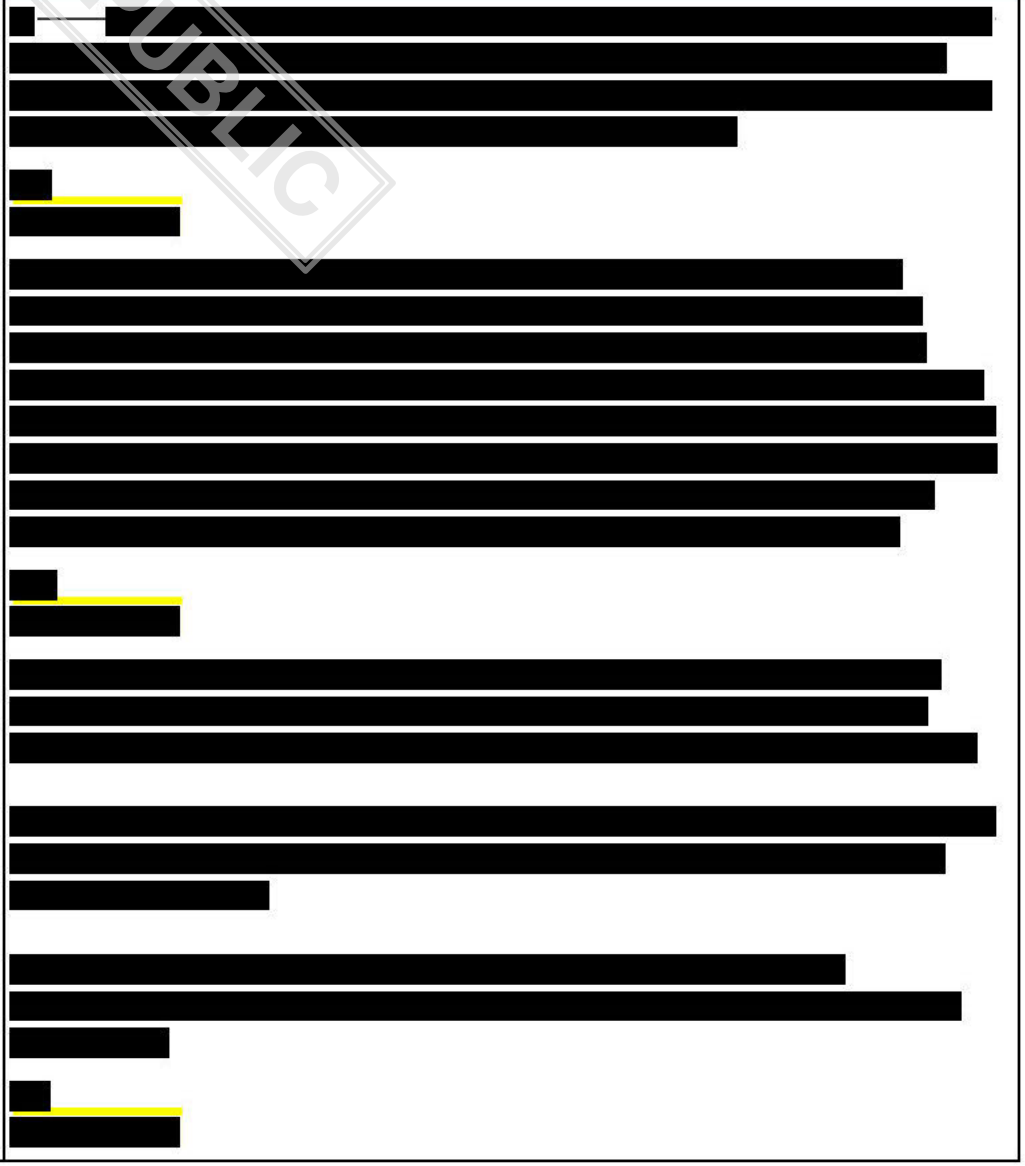
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]
3. Where the Commission has sufficient reason to believe that there is a significant cyber threat for the security of the Union in relation to an ICT supply chain and that action is required to preserve the proper functioning of the internal market, the Commission shall without delay:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

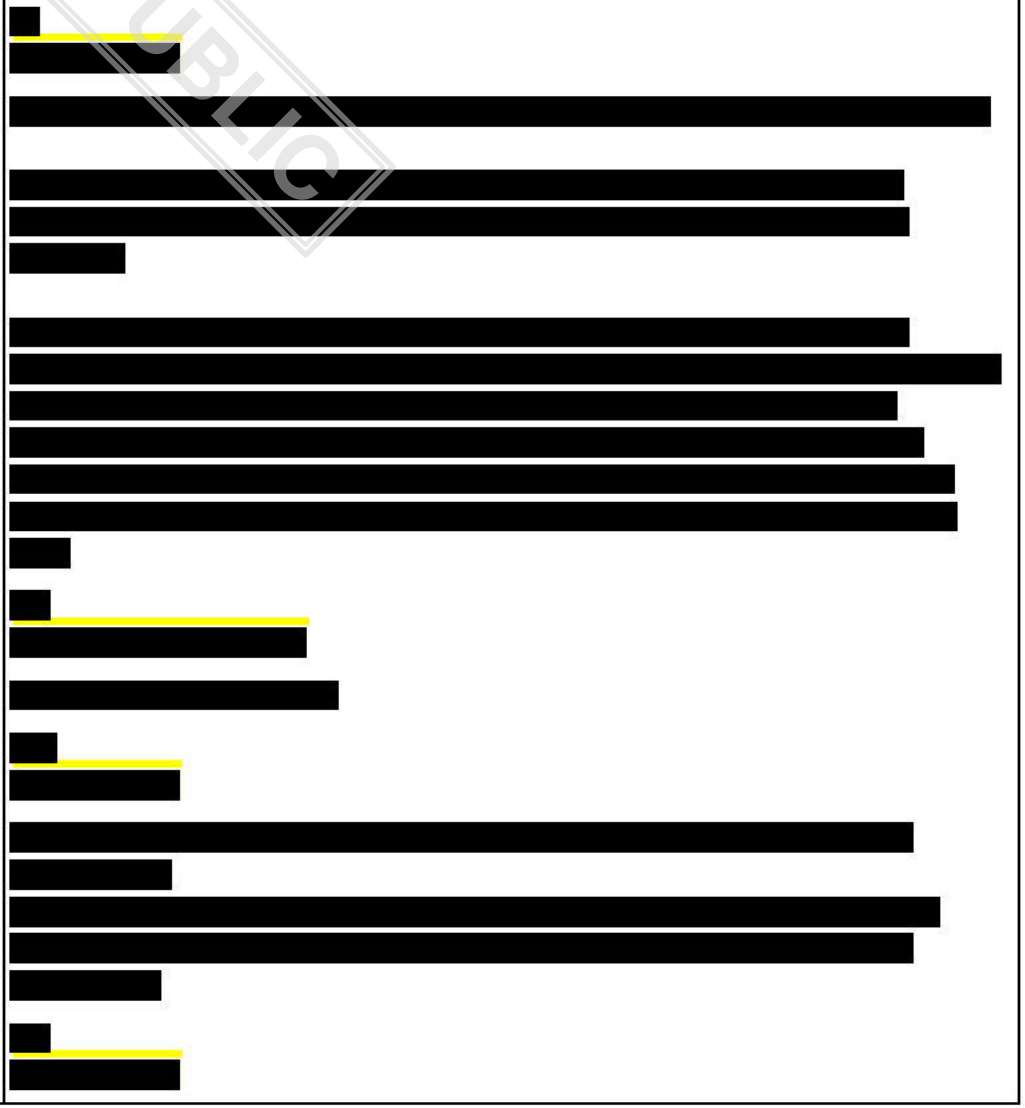
PUBLIC

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) consult the Member States on the need to take one or several of the mitigating measures referred to in Article 103; and	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(b) conduct a security risk assessment, taking into account the consultation of the Member States. The security risk assessment shall include the proposed identification of the key ICT assets as well as the main threat actors, risks and vulnerabilities affecting those assets. The security risk assessment shall develop risk scenarios and propose measures to mitigate the identified risks.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

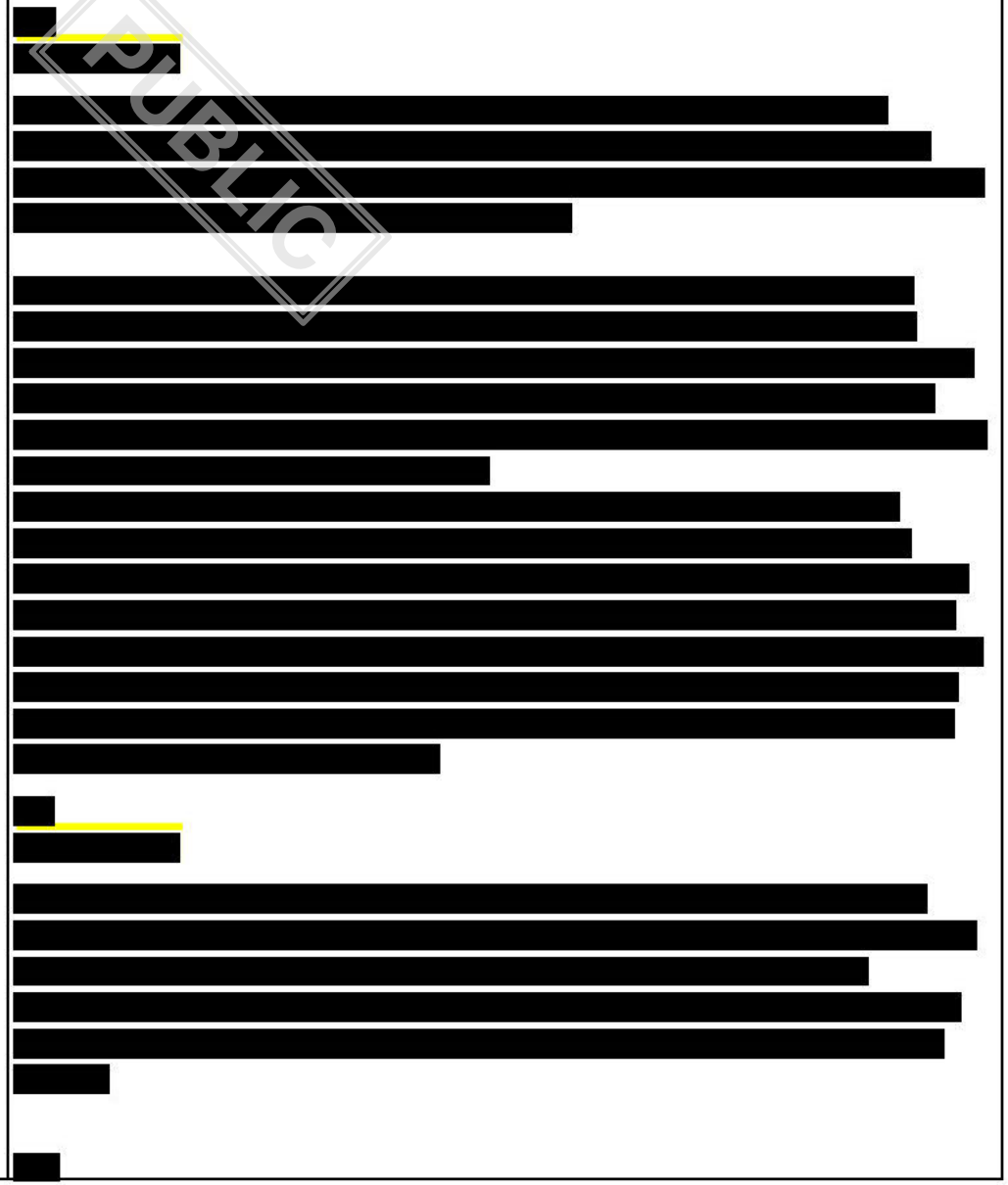
Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 100
Designation of third countries posing cybersecurity concerns



PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. Where, as a result of the security risk assessment referred to in Article 99, or based on other sources, such as a public statement on behalf of the Union or a Member State, it appears that a third country poses a serious and structural non-technical risk to ICT supply chains, the Commission shall verify the risk posed by that country, taking into account the following elements:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

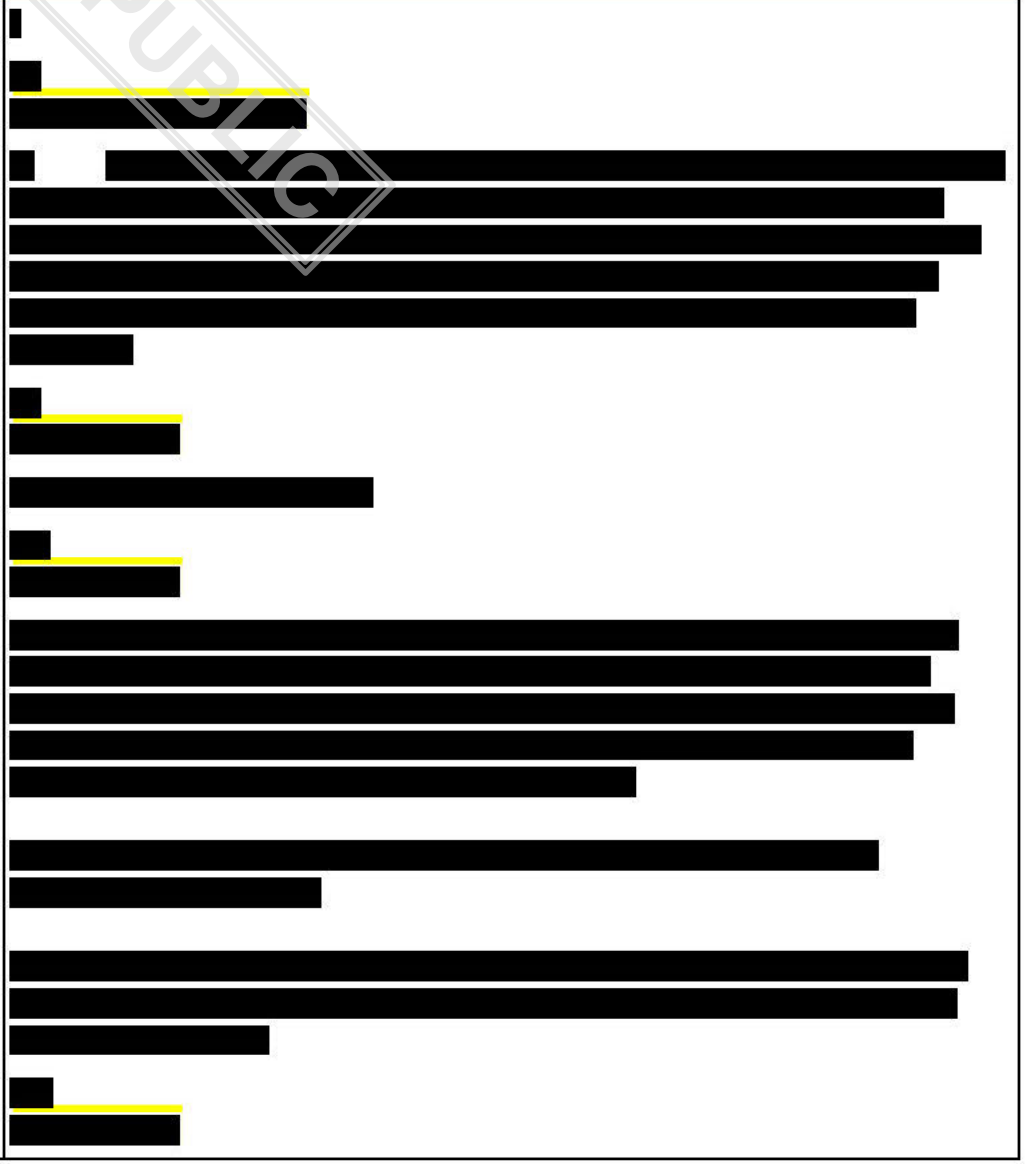
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) the existence of laws in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(b) existing practices in the third country, demonstrated by independent sources, that require entities under the jurisdiction of the third country to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]
(c) the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct the identified security concerns, including about existing practices referred to in point (b);	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(d) substantiated information about one or more incidents of threat actors controlled from that country and operating out of the territory of that country carrying out malicious cyber activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

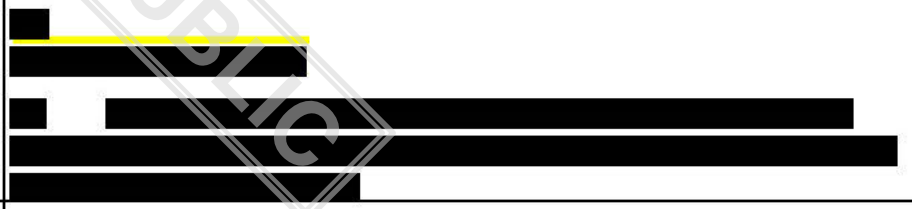
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(e) relevant information stemming from Union-level coordinated security risk assessments or reports by Member States or international organisations.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. When the Commission, following the verification referred to in paragraph 1, concludes that a third country poses serious and structural non-technical risks to ICT supply chains, it may, by means of an implementing act, designate that third country as a country posing cybersecurity concerns to ICT supply chains. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 118(2).	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

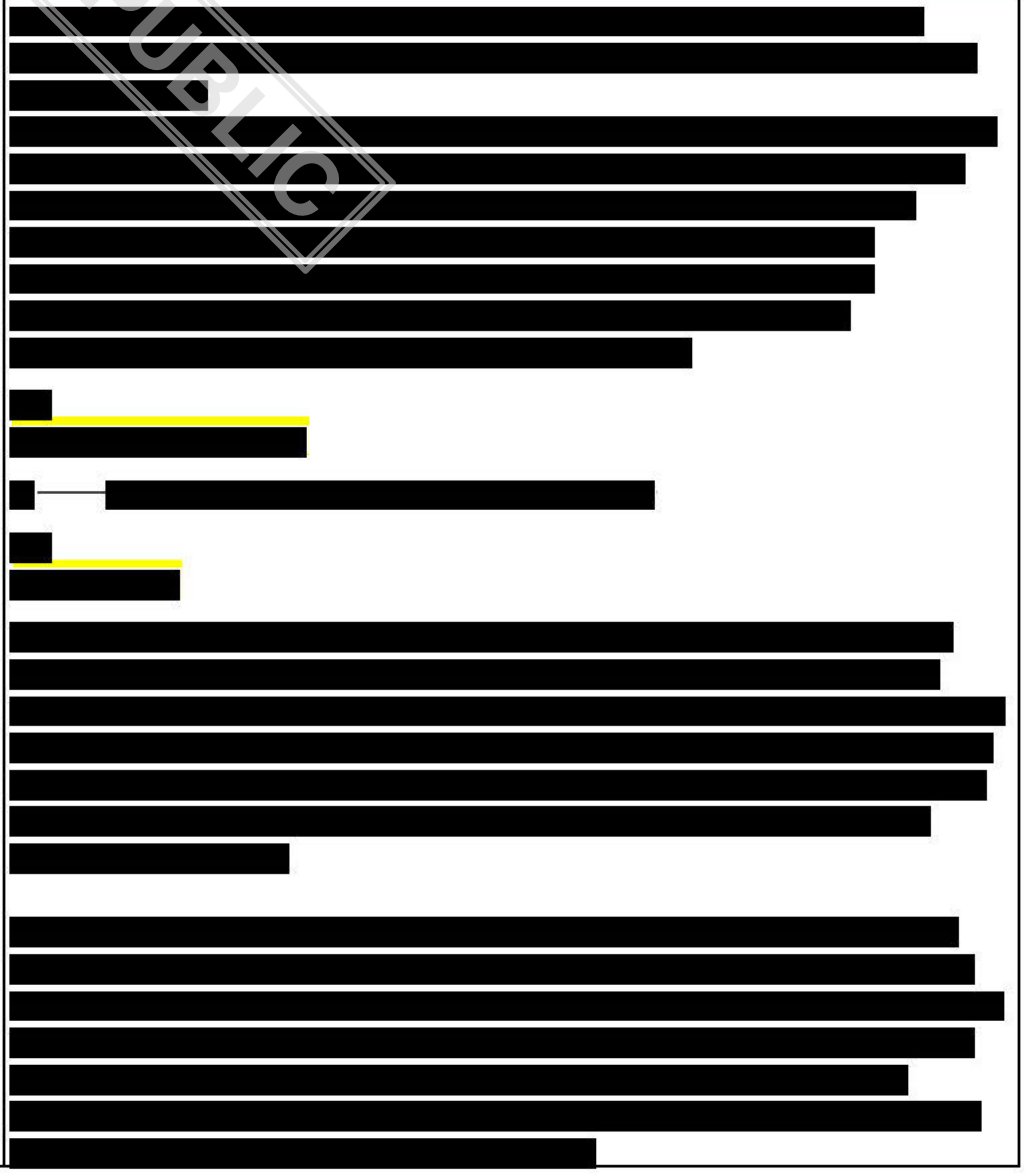
PUBLIC

Commission proposal	Drafting suggestions and Comments
3. The Commission shall review regularly the implementing acts adopted in accordance with paragraph 2.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
4. High-risk suppliers shall not be entitled to:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	

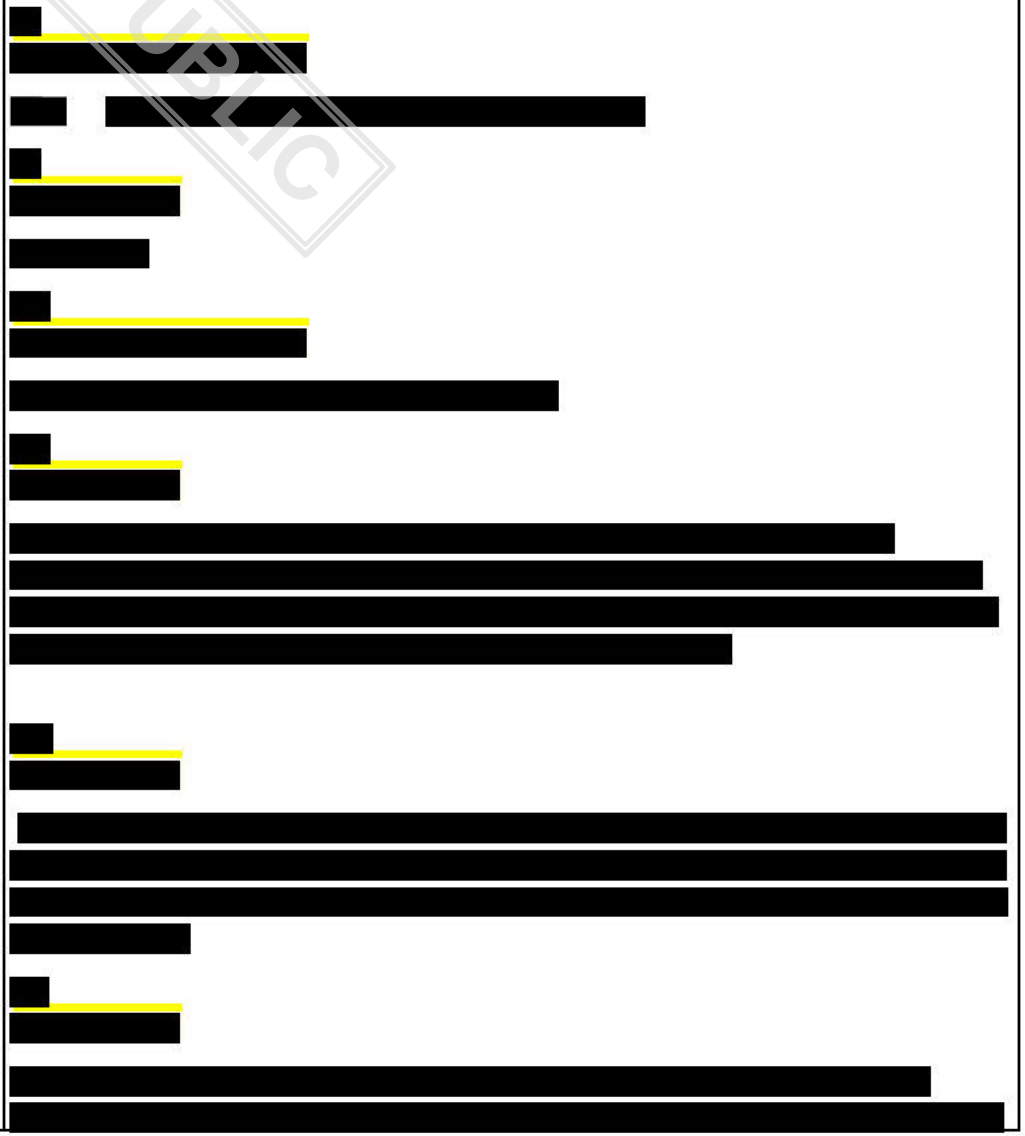
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

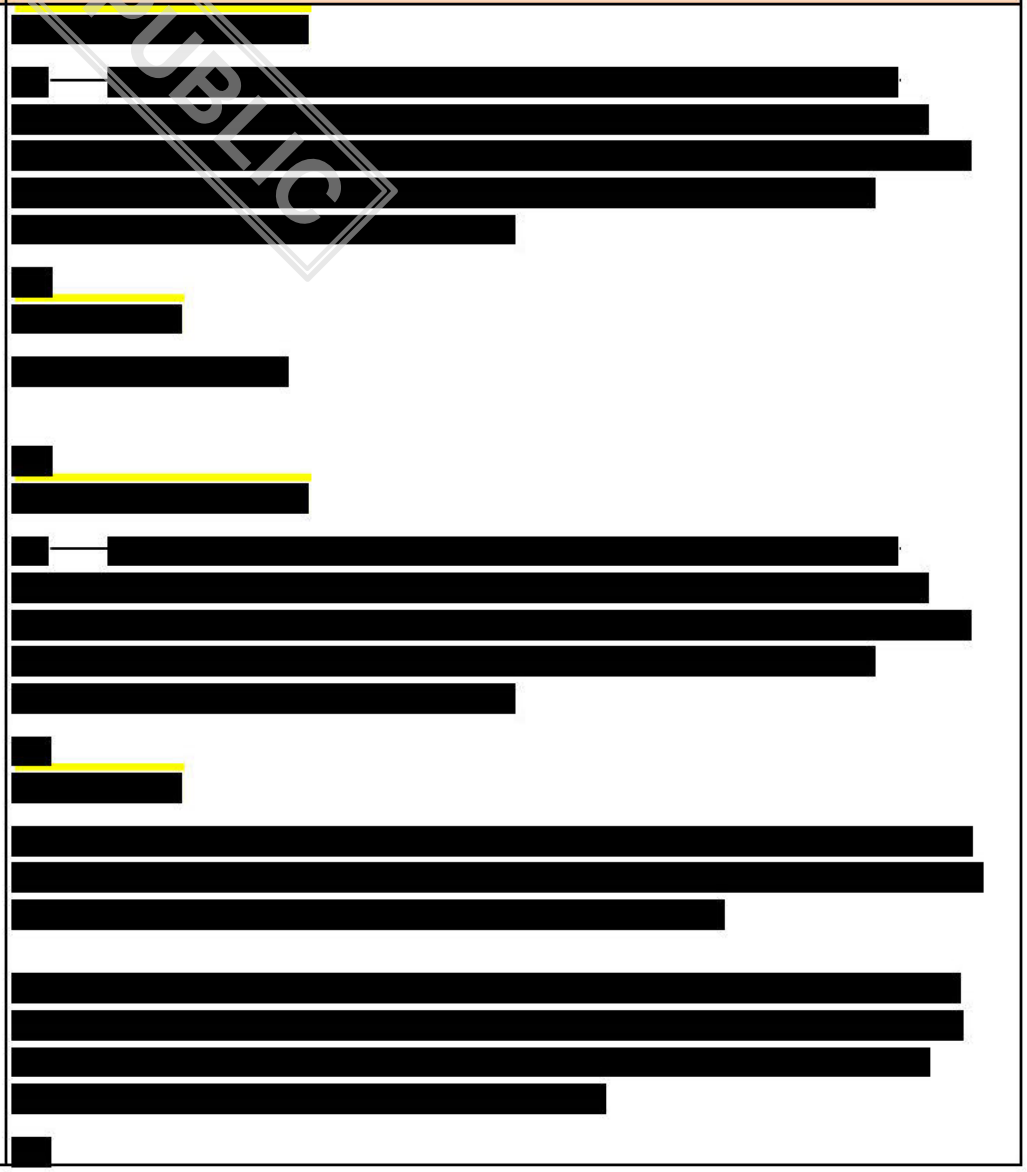
PUBLIC

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]
(a) participate in the development of, assessment, consultation or decisions concerning European standards and European standardisation deliverables referred to in Article 10(1) of Regulation (EU) 1025/2012 and common specifications referred to in Article 27 of Regulation (EU) 2024/2847 in the area of cybersecurity;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(b) apply for or be a holder of any European cybersecurity certificates pursuant to Title III;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(c) become accredited conformity assessment body pursuant to Title III;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(d) apply to become authorised attestation provider of any European individual cybersecurity skills attestations pursuant to Title II, Section 4;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(e) participate in public procurement procedures, organised in accordance with legislation transposing Directive 2014/24/EU and 2014/25/EU in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as identified in accordance with Article 102;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(f) participate in any activities under Union funding programmes and instruments implemented in direct and indirect management in accordance with Article 136 Regulation (EU, Euratom) 2024/2509 and Union sector-specific rules as well as in any Union funding activities implemented in shared management in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as identified in accordance with Article 102.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
The authorities in charge of the procedures referred to in points (a) to (f) shall conduct the necessary assessments for the purpose of this paragraph. The authorities may also rely for this purpose on the list referred to in Article 104.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
5. In cases where a high-risk supplier has already obtained a European cybersecurity certificate pursuant to Title III, the competent authority shall withdraw it without undue delay.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

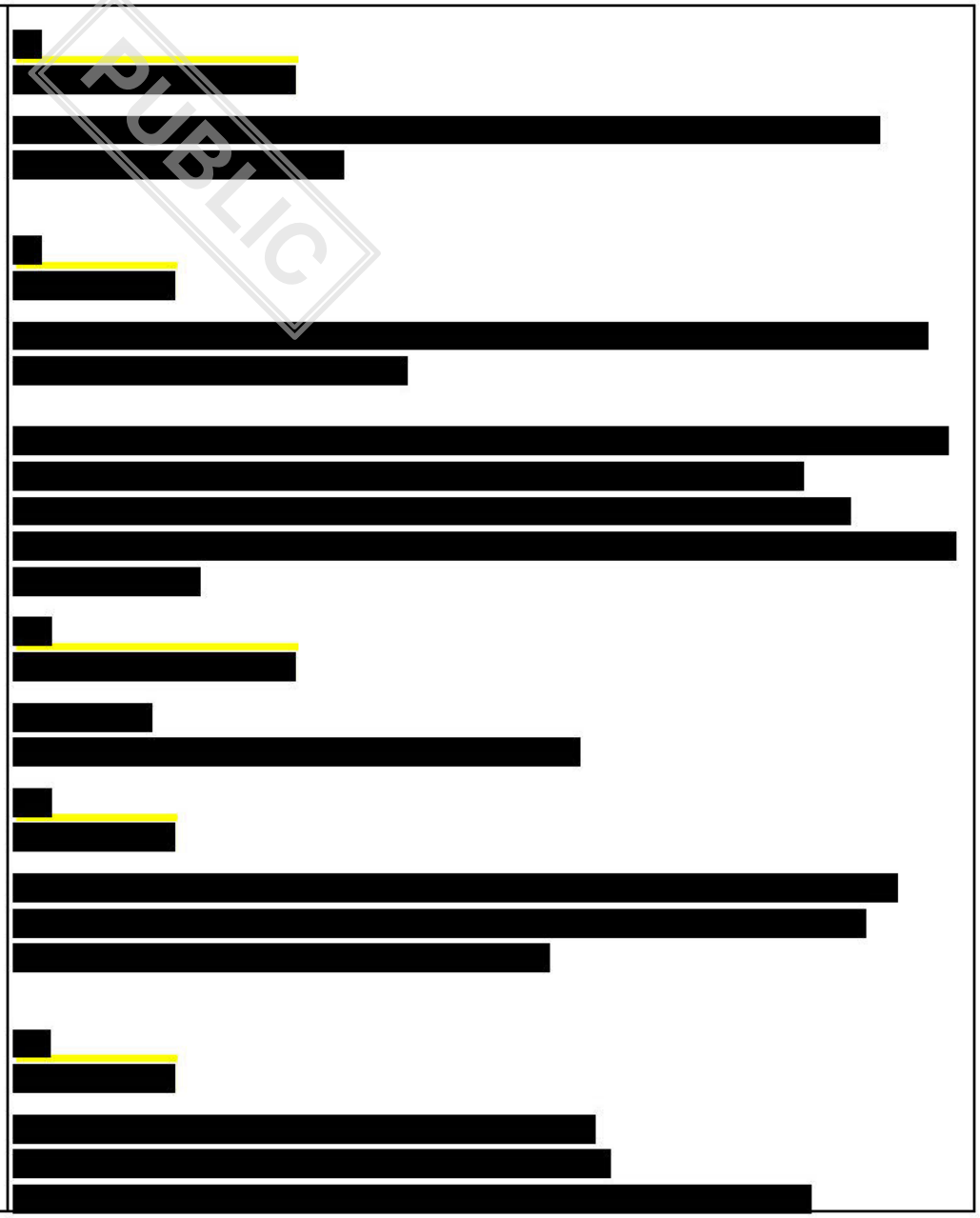
Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

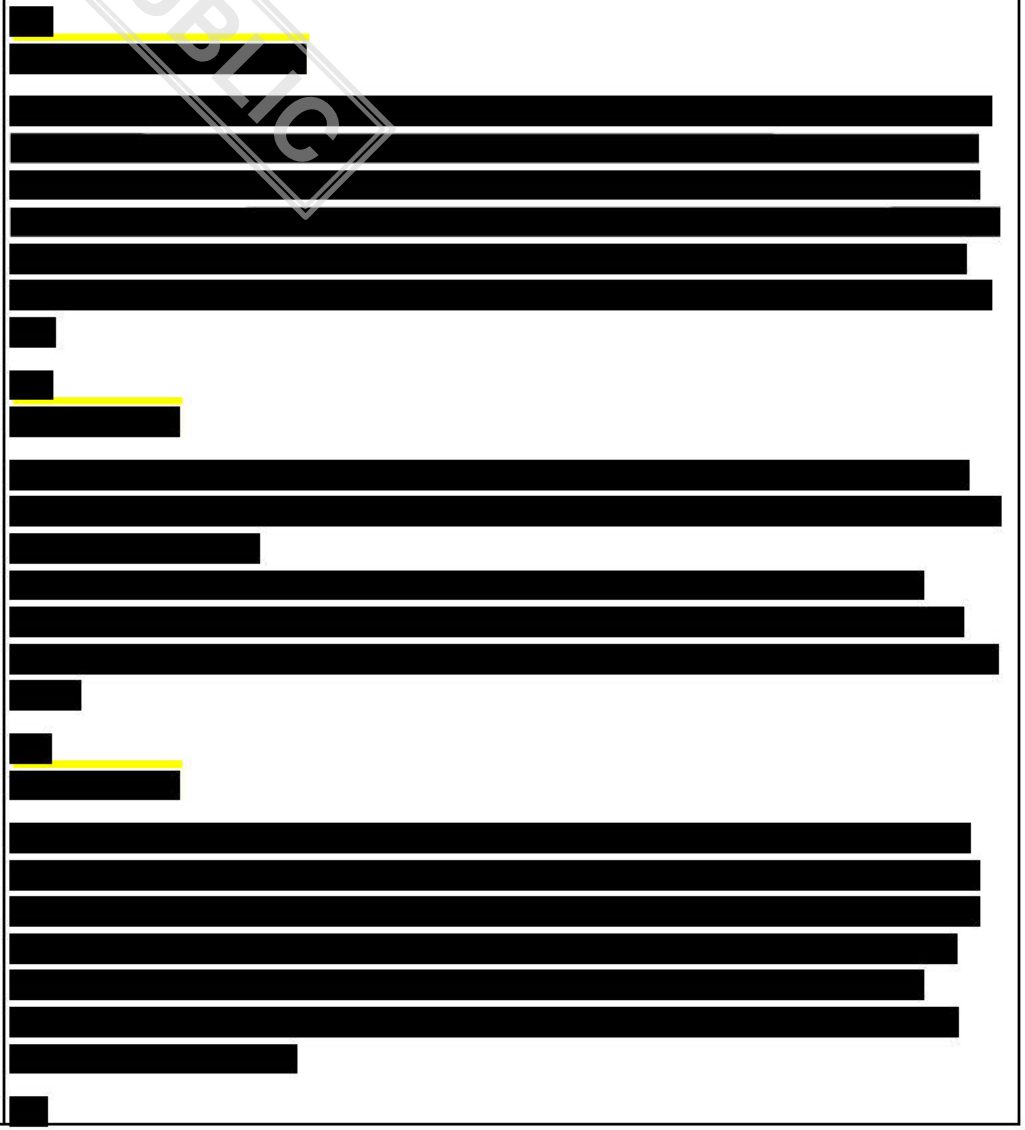
Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 101
General ICT supply chain security mechanism



PUBLIC

Commission proposal	Drafting suggestions and Comments
Where the NIS Cooperation Group has conducted a Union-level coordinated security risk assessment pursuant to Article 99(1) of this Regulation, or after the completion of the procedure in case of significant cyber threat pursuant to Article 99(3) for an ICT supply chain, the Commission may take measures provided for in Articles 102 and 103(1) and (2).	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 102
Identification of key ICT assets

[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. Where the risk assessment conducted in accordance with Article 99(1) or (3) indicates significant cybersecurity risks in relation to an ICT supply chain, the Commission is empowered to adopt implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2) of this Regulation.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. When identifying the key ICT assets referred to in paragraph 1, the Commission shall take into account the following elements:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) whether those assets have essential and sensitive functions for the functioning of products manufactured or services provided by the entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(b) whether incidents, including such caused by exploited vulnerabilities concerning those assets can lead to serious disruptions of ICT supply chains across the internal market or lead to exfiltration of data;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(c) whether there is a dependency on a limited number of suppliers of those assets;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(d) the results of the risk assessments referred to in Article 99.	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

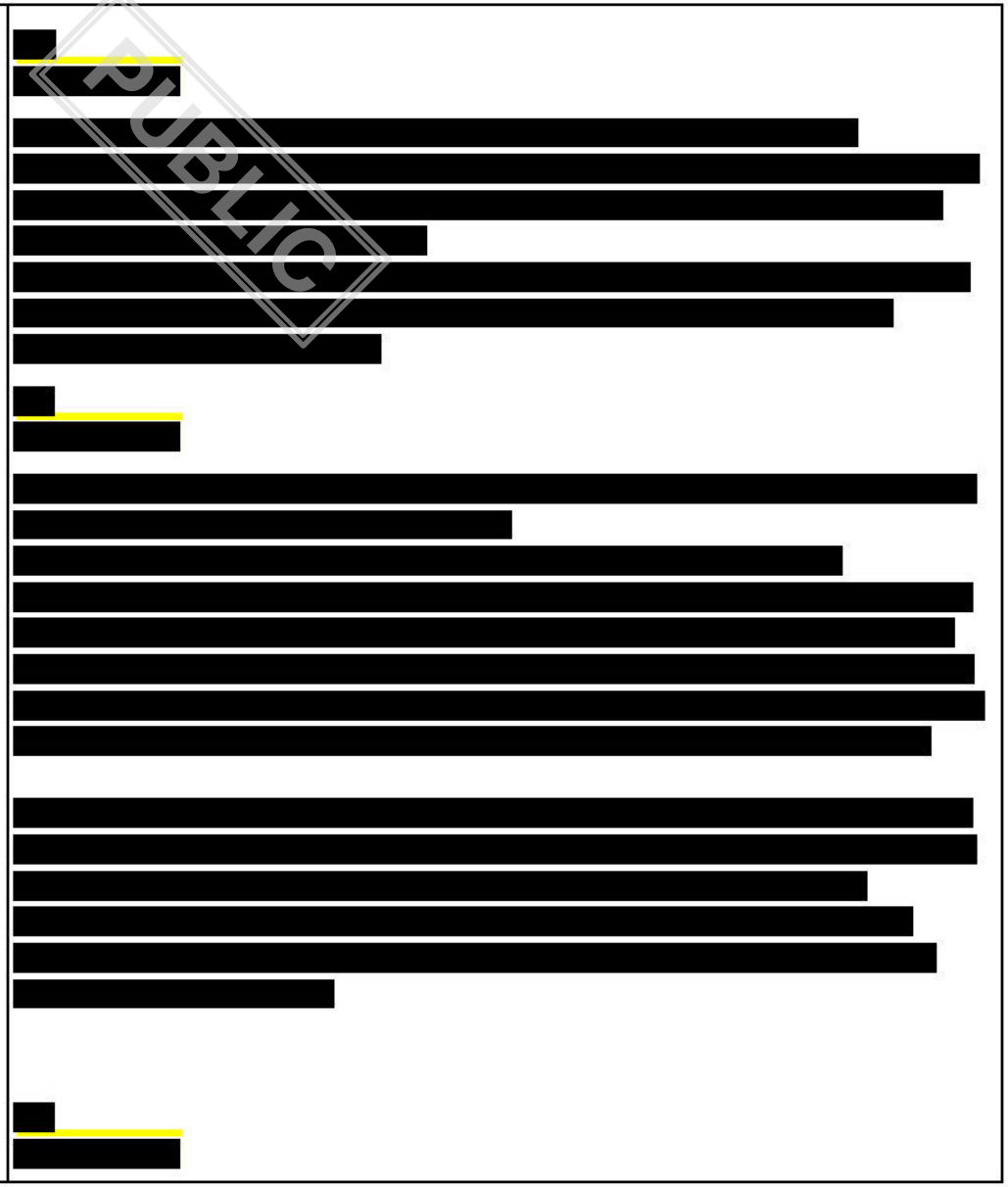
Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 103
Mitigation measures in the ICT supply chain



Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. The Commission is empowered to adopt implementing acts establishing, where necessary to ensure high level of cybersecurity, cyber resilience and trust within the Union, that specific type of entities referred to in Annex I and II to Directive (EU) 2022/2555 shall be prohibited to use, install or integrate in any form ICT components or components that include ICT components from high-risk suppliers as identified in accordance with Article 104 in key ICT assets identified in accordance with Article 102. Such implementing acts shall provide for appropriate transition periods, during which the Commission shall publish the list of high-risk suppliers referred to	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
in Article 104, as well as additional time periods for phasing out the relevant ICT components and components that include ICT components. Such implementing act may also specify these ICT component or components that include ICT components.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. The Commission is empowered to adopt implementing acts establishing, where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, that specific type of entities referred to in Annexes I and II to Directive (EU) 2022/2555 shall be subject to one or several of the following mitigating measures in relation to their ICT supply chain and in particular to key ICT assets identified in accordance with Article 102, to mitigate risks identified in the security risk assessments conducted pursuant to Article 99:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) application of transparency requirements concerning the provision of information to the competent authority about the suppliers in the ICT supply chain for key ICT assets designated in accordance with Article 102;	[redacted]
(b) prohibition related to transfers of data to third countries and remote data processing from a third country;	
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(c) technical measures to be audited by a third party, including:	[redacted]
(i) the use of on-device processing;	
(ii) specific segmentation of network systems;	
(iii) the disabling of any remote or physical access to key ICT assets;	
(iv) the disabling of non-essential features;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
(v) operational network monitoring;	
(vi) testing of hardware and software.	[redacted]
(d) restrictions related to operational control, including outsourcing of organisational functions to managed service providers;	[redacted]
(e) restrictions related to the contractual relations of the entity with its suppliers;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
(f) requirement for the service to be operated, managed, maintained or supported by personnel vetted by the relevant national competent authorities;	[redacted]
(g) diversification of supply of ICT components or components included in ICT components.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
3. When introducing measures referred to in paragraph 2, the Commission may lay down technical and methodological requirements for the measures.	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
4. Before adopting the implementing acts referred to in paragraphs 1 and 2, the Commission shall assess potential risks and dependencies and in particular:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) where applicable, the level of risk associated with the use, installation or integration, in any form, of ICT components or components that include ICT components from high-risk suppliers in key ICT assets;	[redacted]
(b) the potential economic and societal impacts the obligation may have on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(c) the availability of alternative suppliers to high-risk ones;	[redacted]
(d) the potential disruption of cross-border economic and societal activities caused by an incident affecting an entity's ICT supply chain.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
5. The implementing acts referred to in paragraphs 1 and 2 of this Article shall be adopted in accordance with the examination procedure referred to in Article 118(2) and shall be reviewed at least every 36 months.	[redacted]

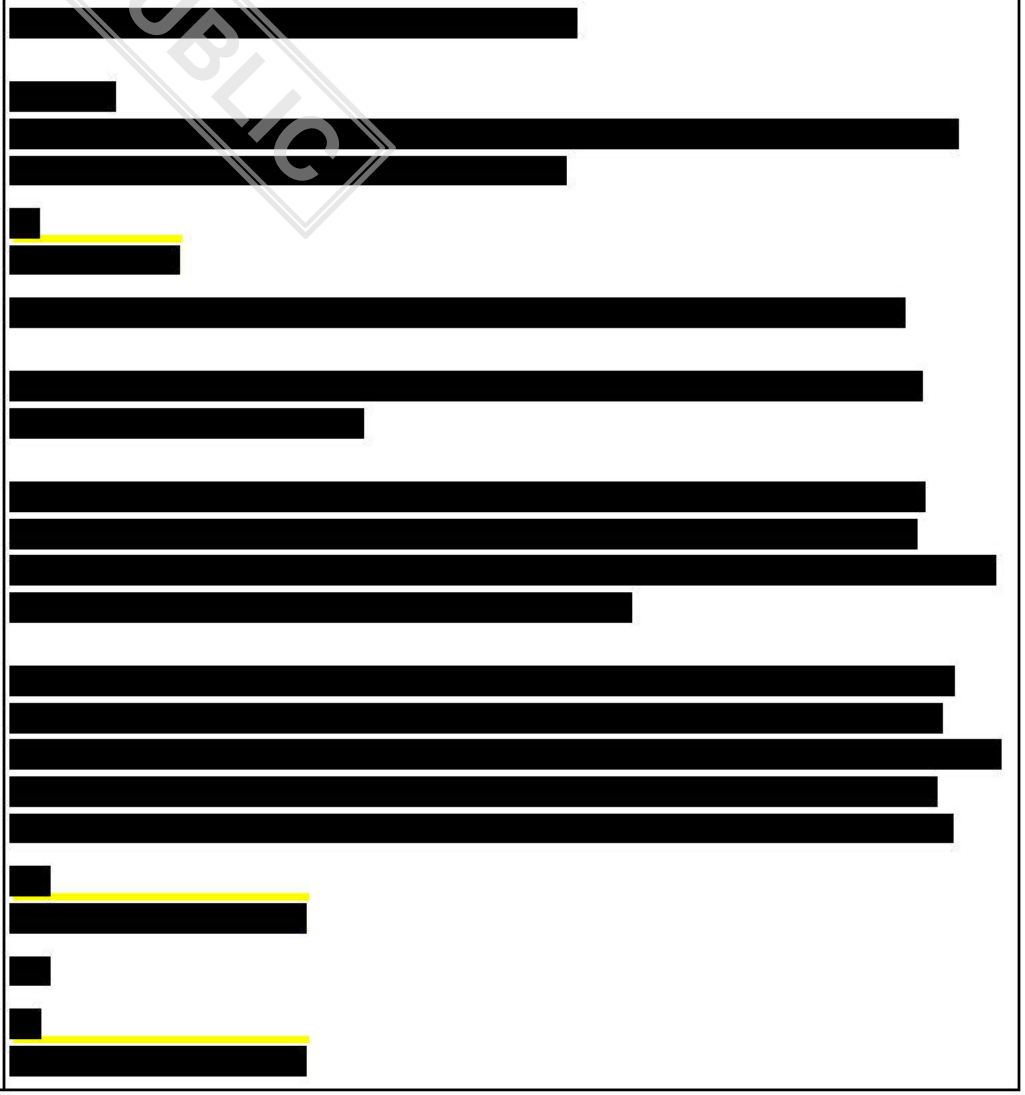
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
6. In exceptional circumstances, which justify an intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the use, installation or integration of ICT components or components that include ICT components from a specific entity established in or controlled by a third country or entities from a third country, or a national from a third country represent a significant non-technical cybersecurity risk for the economic or societal activities of at least three Member States, the Commission shall without delay consult the Member States on the need to take measures at Union level.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
7. The Commission is empowered to adopt implementing acts to establish that specific type of entities referred to in Annexes I and II to Directive (EU) 2022/2555 shall be prohibited to use, install or integrate ICT components or components that include ICT components from an entity referred to in paragraph 6. To that end, it shall consult the entities of the types referred to in Annexes I and II to Directive (EU) 2022/2555 potentially concerned by the	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
prohibition. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2). Where relevant, they shall include appropriate periods for the phasing out of these ICT components or components that include ICT components. Such implementing act may also specify these ICT component or components that include ICT components subject to the prohibition. This prohibition shall also concern ICT components or components including ICT components from all entities controlled by the specific entity referred to in paragraph 6.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
8. The implementing acts referred to in paragraphs (1), (2) and (7) may also specify that the mitigation measures are only applicable to types of entities referred to in Annex I and II to Directive (EU) 2022/2555 of a specific size.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
9. Article 100(4) shall apply to the specific entity established in or controlled by a third country or an entity from a third country, or a national from a third country referred to in paragraph 7.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
10. The implementing acts adopted in accordance with paragraphs (1), (2) and (7) that are applicable to type of entities referred to in Annex I point 10 to Directive (EU) 2022/2555 shall apply mutatis mutandis to the European Institution, bodies, offices and agencies.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 104
Identification of high-risk suppliers

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
1. By way of implementing acts, the Commission shall establish lists of high-risk suppliers relevant for the prohibitions laid down in the implementing acts adopted in accordance with Article 103(1), Article 103(7) or the prohibition referred to in Article 111(1).	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. For that purpose, the Commission shall map the suppliers providing ICT components and components that include ICT components relevant for the prohibition referred to in paragraph 1.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
On this basis, the Commission shall do an initial assessment to identify which of the mapped suppliers are potentially established in a third country designated in accordance with Article 100 or controlled by such third country, by an entity established in such third country or by a national of such third country. The Commission shall also do an initial mapping on suppliers potentially controlled by the entity referred to in Article 103(6).	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
3. The Commission shall assess the place of establishment as well as the ownership and control structure of the suppliers initially identified in accordance with the second subparagraph of paragraph 2.	
4. For the purpose of the assessment referred to in paragraph 3, the Commission shall be entitled to request the necessary information from the suppliers. In case the supplier does not provide the necessary information within the established deadline, the Commission may conclude that the supplier is established in a third country designated in accordance with Article 100 or controlled by such third country, by entities from that third country or by nationals of such third country. Where the Commission is carrying out an assessment for the purpose of Article 103(7) and the supplier does not provide the necessary information within the established deadline, the Commission may conclude that the supplier is controlled by an entity designated in line with that Article. The competent authorities referred to in Article 112 shall also share relevant information with the Commission upon request.	[redacted]

Commission proposal	Drafting suggestions and Comments
	[redacted]

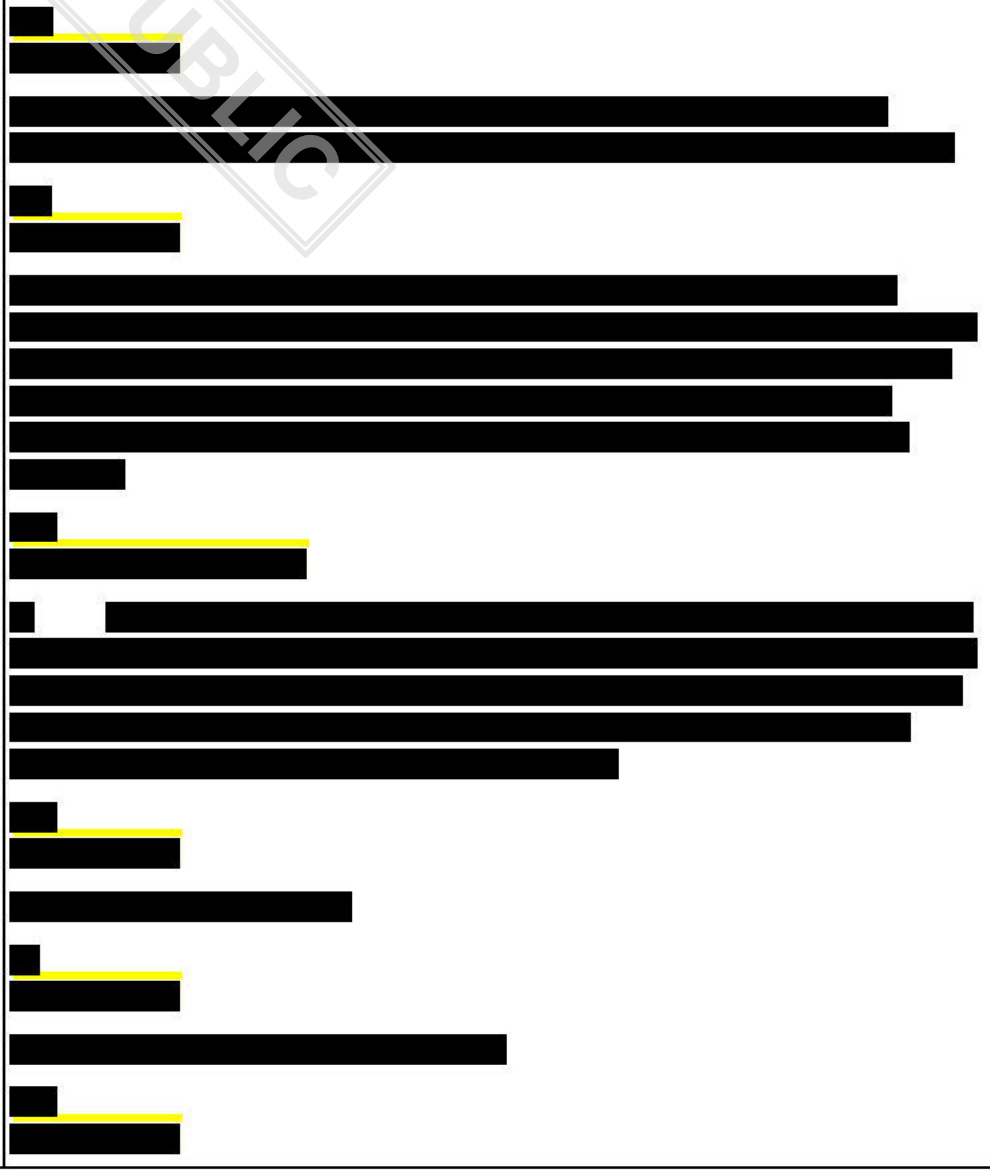
PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
5. The Commission shall share preliminary findings concerning the establishment, control and ownership assessment with the concerned supplier. The Commission shall grant the supplier an opportunity to be heard on those preliminary findings.	[redacted]
6. The Commission may ask a competent authority to carry out the initial establishment, ownership and control assessment of a supplier, where justified in view of the characteristics of the operation of this supplier. A competent	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
authority may offer to carry out such initial assessment. The Commission shall verify these initial findings in view of deciding whether the supplier should be included in the list of high-risk suppliers.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
7. The Commission shall regularly update the list of high-risk suppliers in view of removing or adding high-risk suppliers. High-risk suppliers included in the list may request the Commission to re-assess their establishment, control and ownership structure upon provision of evidence that there have been relevant changes.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
8. Where a competent authority becomes aware, including on the basis of information provided by an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555 that a supplier may need to be included in a list of high-risk suppliers, it shall inform the Commission without undue delay.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 105
Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. An entity established in or controlled by entities from a third country posing cybersecurity concerns designated in accordance with Article 100 may make a reasoned request to the Commission to be exempted:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
(a) from being subject to the prohibition imposed on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 to use, install or integrate in any form its ICT components or components that include its ICT components in key ICT assets of those entities by way of derogation from Article 111 or implementing acts adopted pursuant to Article 103(1);	[redacted]
(b) from being subject to the prohibition to participate in public procurement procedures, organised in accordance with legislation transposing Directive 2014/24/EU and Directive 2014/25/EU in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as defined in accordance with Article 102 in derogation to Article 100(4).	[redacted]

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
2. The request referred to in paragraph 1 shall:	
(a) specify the interest of the entity established in or controlled by entities from a third country posing cybersecurity concerns designated in accordance with Article 100 in being granted the exemption referred to in paragraph 1 of this Article; and	[redacted]

Commission proposal	Drafting suggestions and Comments
	[redacted]
(b) demonstrate with clear evidence that effective mitigating measures will be put in place to address non-technical risks and ensure the absence of any possible exercise of undue interference by the third country designated pursuant to Article 100 in relation to the provision of ICT components or components that include ICT components for the use, installation or integration in key ICT assets of an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
3. The Commission is empowered to adopt implementing acts to further specify the conditions referred to in paragraph 2 point (b), and to lay down detailed rules in respect of the procedures referred to in this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
4. The Commission shall assess the request referred to in paragraph 1 through a fair and transparent process, taking into account:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) the circumstances and additional elements referred to in Article 100(1) and (2) in relation to the designated country posing cybersecurity concerns to ICT supply chains where the entity is established or from where it is controlled;	[redacted]
(b) the effectiveness of the mitigating measures referred to in paragraph 2 point (b);	
(c) whether the exemption for the entity established in or controlled by entities from a third country posing cybersecurity concerns to ICT supply chains would not be detrimental to the Union's interest.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
5. When the Commission, following the assessment in paragraph 3, concludes that it is justified to grant an exemption, it shall do so by way of decision, which it shall notify to the applicant within 9 months of receipt of the request.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
6. When adopting a decision referred to in paragraph 4, the Commission may limit the exemption to a specific period of time and may subject the exemption to conditions for the entity, including:	[redacted]
(a) a timeline for the implementation of mitigating measures referred to in paragraph 2, point (b);	
(b) third-party audits on a regular basis to ensure the effective implementation of mitigating measures;	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(c) reporting obligations regarding compliance.	[redacted]
7. When the Commission, following the assessment in paragraph 3, concludes that it is not justified to grant an exemption, it shall do so by way of a decision, and shall notify it to the applicants within 9 months of receipt of the request.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
8. The Commission may, on its own initiative, withdraw or modify the decision referred to in paragraph 4 in one or more of the following situations:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) there has been a material change in the facts on which the decision was based;	
(b) the entity which has requested the exemption acts contrary to its commitments;	
(c) the exemption was based on incomplete, incorrect or misleading information provided by the entity making the request.	
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
Article 106 *Rights of defence*	[redacted]
The Commission shall ensure that before it adopts an implementing act pursuant to Article 103(7) or before it adopts a decision refusing the granting of exemption pursuant to Article 105(7) on the basis of elements not submitted by the applicant or before it withdraws a decision pursuant to Article 105(8), the entity concerned is given the opportunity of being heard, taking into account the need, in some cases, for an urgency procedure.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
Article 107 *Register*	
The Commission shall maintain a publicly accessible register of its decisions referred to in Article 105(5). The register shall state the names of the entities that have been subject to such decisions. The Commission shall update the register on a regular basis.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 108 *Confidentiality*	[redacted]
Information received by the Commission pursuant to Articles 105 and 106 shall be used only for the purpose for which it was acquired.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 109 *Fees*	
1. The Commission shall levy fees for requests submitted in accordance with Article 105(1).	
2. Fees shall be expressed and payable in euro.	
3. Fees shall be commensurate to the costs linked to the processing of requests referred to in Article 105(1), the assessment of the criteria and information referred to in Article 105(2), and the set-up, maintenance and operation of the register referred to in Article 107. All expenditure of the	

PUBLIC

Commission proposal	Drafting suggestions and Comments
Commission attributed to staff involved in those activities, shall be included in such costs.	[redacted]
4. The Commission shall adopt implementing acts laying down detailed rules relating to the fees, specifying the amount of the fees and the way in which they are to be paid. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	

PUBLIC

Commission proposal	Drafting suggestions and Comments
CHAPTER II ***ICT supply chains in electronic communications networks***	

PUBLIC

Article 110
Key ICT assets for mobile, fixed and satellite electronic communications networks

[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. The key ICT assets for mobile, fixed and satellite electronic communications networks shall be as set out in Annex II.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. ICT components or components that include ICT components provided by high-risk suppliers shall be phased out from the key ICT assets of mobile, fixed and satellite electronic communication networks.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
3. The time period for the phasing out the ICT components or components that include ICT components provided by high-risk suppliers with regard to mobile electronic communications networks shall not exceed 36 months from the publication of the list of high-risk suppliers referred to in Article 104 relevant for the mobile electronic communications networks.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
4. The Commission is empowered to adopt implementing acts in accordance with Article 118(2) to specify the time periods for the phasing out the ICT components or components that include ICT components provided by high-risk suppliers with regard to fixed and satellite electronic communications networks.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
5. The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend Annex II to this Regulation in order to adapt it to technological developments by taking into account the elements referred to in Article 103(4).	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
Article 111 *Prohibitions for mobile, fixed and satellite electronic communication networks*	[redacted]
1. Providers of mobile, fixed and satellite electronic communications networks shall not use, install or integrate, in any form, ICT components or components that include ICT components from high-risk suppliers in the operation of key ICT assets referred to in Annex II.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. In cases where the competent authority designated under this Regulation in a Member State differs from the competent authority pursuant to Regulation (EU) XX/XXXX [DNA proposal], the competent authority designated under this Regulation shall inform without delay the competent authority pursuant to Regulation (EU) XX/XXXX [DNA proposal] about the measures imposed on providers of mobile, fixed and satellite electronic communications networks in accordance with Article 114. The authorities shall ensure close cooperation for the purposes of effective supervision and enforcement of those measures.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
CHAPTER III ***Competent authorities, supervision and enforcement, jurisdiction, rights of defence***	
Article 112 *Competent authorities*	
1. Each Member State shall designate the competent authorities referred to in Article 8 of Directive (EU) 2022/2555 as authorities responsible for taking the supervisory and enforcement measures referred to in Article 114.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. Competent authorities shall be structurally and functionally fully impartial and free from any external influence, whether direct or indirect; in particular they shall neither seek nor take instructions from any other public authority or any private party.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
3. Member States shall ensure that their competent authorities have appropriate powers, sufficient human and technical resources and relevant expertise to effectively carry out the supervisory and enforcement measures referred to in Article 114.	[redacted]
4. Each Member State shall without undue delay notify the Commission of the names of the competent authorities designated in accordance with paragraph 1, of the respective tasks of those authorities and of any subsequent changes thereto. Each Member State shall also make public the names of the competent authorities designated in accordance with paragraph 1.	
Article 113 *Network for cooperation and support services of the Commission*	
In view of effective supervision, the Commission shall set up a network for cooperation of competent authorities of Member States referred to in Article 112 and the Commission to serve as a platform for cooperation and exchange of information, in particular for the purpose of the establishment, control and ownership assessment referred to in Article 104. The Commission shall provide the administrative support to the network.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 114
Supervisory and enforcement measures

[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. The competent authorities as referred to in Article 112 are entitled to take the supervisory and enforcement measures on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Member States shall	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
ensure that the abovementioned measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case. Member States shall notify the Commission of the rules enacted to that end and their subsequent amendments.	[redacted]
2. When exercising their supervisory tasks in relation to entities referred to in Annexes I and II to Directive (EU) 2022/2555, competent authorities are entitled to subject those entities to the following:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) requests for a detailed and up-to-date list of their relevant suppliers and service suppliers;	[redacted]
(b) requests to access data, documents and information necessary to verify compliance with this Regulation;	
(c) on-site inspections and off-site supervision, including random checks conducted by trained professionals;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(d) requests regarding the composition of hardware or software products installed or integrated in any form into the network or system, including components and transitive dependencies, in a commonly used and machine-readable format.	[redacted]
3. When exercising their enforcement powers in relation to entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555, competent authorities are entitled to:	[redacted]
(a) issue warnings about infringements of this Regulation by the entities concerned, setting out the relevant facts and legal considerations;	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(b) adopt decisions requiring the entities concerned to remedy the infringement of this Regulation or the deficiencies identified in the implementation of mitigating measures;	
(c) order the entities concerned to cease activities that infringe this Regulation and desist from repeating such activities; and	
	[redacted]
(d) impose penalties, in accordance with the rules relates to the amount laid down in Article 115 or request the imposition of such penalties by the relevant bodies, courts or tribunals, in accordance with national law.	
4. When taking any of the enforcement measures referred to in the previous paragraph, the competent authorities shall consider the circumstances of each individual case and take due account of the following factors:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) the seriousness of the infringement and the importance of the provisions breached;	[redacted]
(b) the duration of the infringement;	[redacted]
(c) the turnover of the relevance of the entity concerned;	[redacted]
(d) any relevant previous infringement by the entity concerned;	[redacted]
(e) where applicable, any material or non-material damage caused by the infringement, including any financial or economic loss, effects on other entities and the number of users affected;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(f) any intent or negligence on the part of the entity concerned;	[redacted]
(g) any measures taken by the entity to prevent or mitigate the material or non-material damage;	[redacted]
(h) the level of cooperation with the competent authorities of the natural or legal persons held responsible.	[redacted]
For the purposes of the first subparagraph, point (a), the following shall constitute serious infringement:	[redacted]
(i) repeated violations;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
(j) failure to notify or remedy significant incidents;	
(k) failure to remedy deficiencies following binding instructions from competent authorities.	
competent authorities shall notify the entities concerned of their preliminary findings before taking enforcement measures. The entities concerned shall be given a reasonable time to submit observations on the preliminary findings. The competent authorities shall set out detailed reasoning for their enforcement measures.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
6. The competent authorities shall respect the principles of confidentiality and of professional and commercial secrecy.	[redacted]
7. The competent authorities shall cooperate with each other and with the Commission for the purposes of supervision and enforcement under this Title in accordance with Article 116.	
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 115 *Penalties*	[redacted]
1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
2. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendments affecting them.	
3. Penalties shall be imposed in addition to any of the measures referred to in Article 114(3), points (a), (b) and (c).	
4. When deciding whether to impose a penalty and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the factors referred to in Article 114(4) first subparagraph..	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
5. Infringements of Article 103(2), point (a), shall, in accordance with paragraph 3 of this Article, be subject to penalties of a maximum of 1 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.	[redacted]
6. Infringements of Article 103(2), points (b) to (g), shall, in accordance with paragraph 3 of this Article, be subject to penalties of a maximum of 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
7. Infringements of Article 103(1), and of Article 111 shall, in accordance with paragraph 3, of this Article be subject to penalties of a maximum of 7 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 116 *Mutual assistance*	[redacted]
1. Where an entity of the type referred to in Annexes I or II to Directive (EU) 2022/2555 provides services in more than one Member State, or provides services in one or more Member States and its key ICT assets are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with each other and the Commission and shall assist each other and the Commission with a view to ensuring the effective and efficient application of the Regulation. To that end, the following rules shall apply as a minimum:	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(a) the competent authorities applying supervisory or enforcement measures in a Member State shall inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken;	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
(b) a competent authority in a Member State may request another competent authority in another Member State to take supervisory or enforcement measures;	[redacted]
(c) a competent authority in a Member State shall, upon receipt of a substantiated request from another competent authority in another Member State, provide that other competent authority with mutual assistance, on a best-efforts basis, so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
2. The mutual assistance referred to in paragraph 1, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission.	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
3. Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.	[redacted]
4. In view of the obligation to comply with the principles of confidentiality and of professional and commercial secrecy as referred to Article 114(6), any information exchanged in the context of a request for assistance and provided pursuant to this Article shall be used only in respect of the matter for which it was requested.	[redacted]
	[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]

PUBLIC

Article 117
Jurisdiction and territoriality

[redacted]

PUBLIC

Commission proposal	Drafting suggestions and Comments
	[redacted]
1. Entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555 falling within the scope of this Regulation shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of:	
(a) providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;	
(b) DNS service providers, top-level-domain (TLD) name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service	

PUBLIC

Commission proposal	Drafting suggestions and Comments
providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;	
(c) public administration entities, which shall be considered to fall under the jurisdiction of the Member State to which they belong;	
(d) air carriers, which shall be considered to fall under the jurisdiction of the Member State whose competent licensing authority granted the operating licence to the entity pursuant to Regulation (EC) No 1008/2008 of the European Parliament and of the Council[1], or, where the operating licence or equivalent has not been granted in accordance with that Regulation, they shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2. 1 Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (Recast) (OJ L 293, 31.10.2008, p. 3-20, ELI: https://eur-lex.europa.eu/eli/reg/2008/1008/oj/eng).	[redacted]

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
2. For the purposes of this Regulation an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where most of the cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.	
3. If an entity of a type referred to in Annexes I and II to Directive (EU) 2022/2555, is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. Where such an entity is an entity as referred to in paragraph 1, point (a), it shall be considered to fall under the jurisdiction of the Member State in which it provides its services. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Regulation.	[redacted]
4. The designation of a representative by an entity referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
5. Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned where the entity provides services or has a network and information system on their territory.	
TITLE VI **FINAL PROVISIONS**	
Article 118 *Committee procedure*	FI (Comments): Paramount provision on committee procedure. FI would like more information on the committee procedures and why they are considered to be the right instrument for involving Member States. PL (Comments): Poland suggests to rely on the Council decisions instead of comitology. Therefore Articles 118 and 199 are not necessary.
1. The Commission shall be assisted by a committee. That committee shall have two configurations. In respect of Titles II and III, the Commission shall be assisted by a committee in the first configuration, whereas in respect of Title IV, the Commission shall be assisted by a committee in the second configuration. That committee shall be committee within the meaning of Regulation (EU) No 182/2011.	FR (Drafting suggestions): 1. The Commission shall be assisted by a committee. That committee shall have two configurations. In respect of Titles II and III, the Commission shall be assisted by a committee in the first configuration, whereas in respect of Title IV, the Commission shall be assisted by a committee in the second

Commission proposal	Drafting suggestions and Comments
	configuration. That committee shall be committee within the meaning of Regulation (EU) No 182/2011. **1a. Where implementing acts are adopted pursuant to this Regulation, they shall be adopted in accordance with the examination procedure referred to in Article 118(2).** **1aa. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.** **1aaa. Where the committee delivers no opinion within the meaning of Article 5(4) of Regulation (EU) No 182/2011, the Commission shall not adopt the draft implementing act.** FR (Comments): French authorities insist on the need to add this clarification on applicable procedures as Member States should have a more proeminent role in the mechanism established by title IV of this Regulation.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	DK (Drafting suggestions): **Where reference is made to this paragraph, point (b) of Article 5(4) of Regulation (EU) No 182/2011 shall apply.** DK (Comments): DK: The Commission has removed the reference to has removed Article 5, paragraph 4, litra b in Regulation (EU) no. 182/2011, (comitology). We would like to use the same formulation as in CSA 1. DK finds it important to ensure real inclusion and possibility of control by member states in the process of delegated decisions.

Commission proposal	Drafting suggestions and Comments
	IT (Drafting suggestions): 2. Where reference is made to this paragraph, **point (b) of** Article 5**(4)** of Regulation (EU) No 182/2011 shall apply. IT (Comments): This is to reinstate the same procedure in place for the current cybersecurity act and ensure that the adoption of implementing acts follows an agreement among Member States, especially in view of the significant implications that decisions taken both Title III and IV may have national security related aspects. PL (Comments): As discussed in the previous comments, Poland does not agree to the implied approval of the implementing regulations (Article 5(4) of the Regulation (EU) No 182/2011). The procedure must be clearly described in this Regulation.
Article 119 *Exercise of the delegation*	PT (Drafting suggestions): ~~Article 119~~ ~~Exercise of the delegation~~ PT (Comments): To maintain the position regarding article 80.º

Commission proposal	Drafting suggestions and Comments
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	PT (Drafting suggestions): ~~1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.~~
2. The power to adopt delegated acts according to Articles 80(2) and Article 110(5) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	PT (Drafting suggestions): ~~2. The power to adopt delegated acts according to Articles 80(2) and Article 110(5) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.~~
3. The delegation of power referred to in Articles 80(2) and Article 110(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	PT (Drafting suggestions): ~~3. The delegation of power referred to in Articles 80(2) and Article 110(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.~~
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.	PT (Drafting suggestions): ~~4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.~~

Commission proposal	Drafting suggestions and Comments
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	PT (Drafting suggestions): ~~5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.~~
6. A delegated act adopted pursuant to Articles 80(2) and Article 110(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	PT (Drafting suggestions): ~~6. A delegated act adopted pursuant to Articles 80(2) and Article 110(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.~~
Article 120 *Evaluation and review*	DK (Comments): DK: The evaluation of CSA 1 was delayed quite substantially. We suggest to add safeguards in article 120 to ensure that the Commission will conduct the evaluation before the deadline in the text. We would welcome suggestions from Council Legal Service.
1. By [DD MM YYYY], and every five years thereafter, the Commission shall commission an evaluation which shall be conducted in accordance with the Commission's guidelines.	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
2. The evaluation referred to in paragraph 1 shall include an assessment of the following:	
(a) ENISA's performance in relation to its objectives, mandate, mission, tasks, governance and location;	
(b) the effectiveness, efficiency and EU added value of the European individual cybersecurity skills attestations schemes as laid down in Title II, Chapter II, Section 4 of this Regulation;	
(c) the impact, effectiveness and efficiency of the provisions of Title III of this Regulation with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services, ICT processes, managed security services and entities in the Union and improving the functioning of the internal market;	
(d) the impact, effectiveness and efficiency of provisions of Title IV of this Regulation with regard to the objectives of the trusted ICT supply chain framework.	AT (Comments): On the basis of which criteria/KPIs will COM evaluate the impact, effectiveness and efficiency of the provisions of Title IV? Such criteria/KPIs should be included in the legal text.
3. The evaluation referred to in paragraph 1, point (a), shall, in particular, address the possible need to modify the mandate of ENISA, and the financial implications of any such modification.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
4. On the occasion of every second evaluation, referred to in paragraph 1, point (a), the Commission shall assess the results achieved by ENISA having regard to its objectives, mandate, mission, governance and tasks, including an assessment of whether the continuation of ENISA is still justified with regard to these objectives, mandate, mission, governance and tasks.	
5. The Commission shall report to the European Parliament, the Council and the Management Board on the evaluation findings. The findings of the evaluation shall be made public.	
Article 121 *Repeal and continuation of activities*	
1. Regulation (EU) 2019/881 of the European Parliament and of the Council is repealed with effect from DDMMYYYY.	
2. References to Regulation (EU) 2019/881, ENISA and European cybersecurity certification schemes as established by that Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table set out in Annex III to this Regulation.	
3. ENISA as governed by this Regulation shall continue operations and activities of ENISA as established by Regulation (EU) 2019/881 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities. All decisions of the Management Board and the	

Commission proposal	Drafting suggestions and Comments
Executive Board adopted in accordance with Regulation (EU) 2019/881 shall remain valid, provided that they comply with this Regulation.	
4. The Executive Director appointed pursuant to Article 15(1), point (n) of Regulation (EU) 2019/881 shall remain in office and exercise the tasks and responsibilities of the Executive Director as referred to in Article 32 of this Regulation for the remaining part of the Executive Director's term of office. The other conditions of their contract shall remain unchanged.	
5. The candidate schemes whose preparation was requested pursuant to Article 49 of Regulation (EU) 2019/881 shall be considered to have been requested pursuant to the corresponding provisions of this Regulation. The provisions of Title III of this Regulation shall apply to those candidate schemes accordingly.	
6. The members of the Management Board appointed by the Commission and alternate members appointed pursuant to Article 14 of Regulation (EU) 2019/881 shall remain in office and exercise the functions of the Management Board as referred to in Article 27 of this Regulation for the remaining part of their term of office. The members of the Management Board appointed by Member States pursuant to Article 14 of Regulation (EU) 2019/881 shall remain in office and exercise the functions of the Management Board as referred to in Article 27 of this Regulation provided that they hold functions referred to in Article 24(3) of this Regulation.	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 122 *Entry into force*	
This Regulation shall enter into force on the […] day following that of its publication in the *Official Journal of the European Union*.	
This Regulation shall be binding in its entirety and directly applicable in all Member States.	