Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2026/0011 (COD)

Brussels, 17 July 2026

WK 10695/2026 INIT

LIMITE

CYBER

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

WORKING DOCUMENT

From: To:	Presidency Horizontal Working Party on cyber issues (attachés)
N° Cion doc.:	ST 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): Title IV: Security of ICT Supply Chains: Guiding questions

Delegations will find attached the Presidency's guiding questions for the discussion on the security of ICT Supply Chains.

PUBLIC

CYBERSECURITY ACT 2 (CSA 2): Title IV ICT Supply Chain Guiding Questions

Introduction:

The Commission proposal for the Cybersecurity Act 2 (CSA2) was released on 20 January 2026 and the HWPCI has carried out the initial article-by-article read through under the CY Presidency. Member States highlighted many areas in Title IV on the ICT Supply Chain that would require more discussion and clarification.

Member States submitted written comments that were received on 29 June under the CY Presidency. Based on these written comments, bilateral engagement with Member States through the speed dating process, and an initial brainstorming session with the Commission on July 14, the IE Presidency has identified key areas that it wishes to open discussions on:

- The Scope of the ICT supply chain mechanism and structure of the mechanism;
- Decision-making mechanisms in the designation of third countries posing cybersecurity concerns;
- Procedures to designate High Risk Suppliers.

To this end, the Presidency has created the following guiding questions to get a clearer direction of travel for the purpose of drafting a REV1 text, with a view of clarifying the underlying principles of the mechanism for addressing ICT supply chain risks.

The Presidency plans to present these questions at the HWPCI meeting on 20 July and to have a first exchange of views on these questions at the HWPCI scheduled for Monday 07 September. Written comments on the guiding questions are welcomed by Wednesday 09 September COB. Responses to these guiding questions at the HWPCI meeting on 07 September and in writing on 09 September, along with the previous written comments on the ICT Supply Chain (Title IV) received on 29 June, will structure and inform the REV1 text that will follow soon after.

1) Scope and Methodology

Background:

Member States wish to understand the scope of the ICT supply chain mechanism. While the scope of the proposal gives the Commission and Member States a wide-ranging ability to address vulnerabilities in the supply chain at Union level, it also raises the question of whether it should require greater Member State involvement in the approval process of any action taken. Further defining the scope could provide greater clarity and offer Member States greater predictability regarding the regulation's boundaries but it will also limit the ability and extent of the Commission and Member States in securing the entire supply chain.

While the Commission's proposed scope (Article 98) is grounded in the sectors listed in Annexes 1 and 2 of the NIS2 Directive, it broadens this approach to encompass entities 'of the type' referred to in Annexes 1 and 2 of NIS2, regardless of their organisational size. This entails coverage also of SMEs operating in the NIS2 sectors that might not meet the thresholds to come under NIS2, but still provide critical ICT assets to Important and Essential Entities.

Article 99 outlines the framework for security assessments to identify risks to Key ICT Assets and Supply Chains under Title IV. Under the standard procedure, these assessments are conducted by the NIS Cooperation Group upon the request of the Commission or a group of at least three Member States. However, to address urgent cyber threats to the internal market, Article 99(3) also establishes a direct pathway enabling the Commission to independently conduct these assessments following consultation with Member States.

Question 1 - Do you believe only applying the scope of the framework (Article 98) to address **non-technical** risks to just the entities listed in Annexes 1 & 2 of the NIS2 Directive is sufficient? Does it adequately capture the range of entities that could supply key ICT assets, or components of key ICT assets, in critical ICT Supply Chains to Important and Essential Entities?

Question 2 - Do you believe that the criteria for the Security Risk Assessments set out in Article 99 are sufficient? Should they be further developed or would you like to see a common risk methodology for non-technical risks applied to the security risk assessments?

PUBLIC

2) The designation of third countries posing cybersecurity concerns

PUBLIC

Background:

Member States have flagged that the Country of Concern designation in Article 100 has wide-ranging potential consequences, which may warrant a tailored approach. While Article 105 introduces an important appeal mechanism for individual entities affected by an Article 100 decision, further consideration may be needed to fully address the wider impacts of a country-wide designation.

The Presidency has explored potential options to address this. It has identified that an assessment of impact and potential for greater Member State involvement could be a way forward. The scope of Article 100 is broadly defined, and the designation of third countries can be triggered in two separate ways:

1. As a result of a security risk assessment conducted under Article 99, or
2. Based on other sources such as public statements made by Member States or on behalf of the Union

If either of the above leads to an appearance that a third country poses a serious and structural non-technical risk to ICT supply chains, the Commission is obliged to verify the risk posed by the country by taking into account a set of elements listed in Article 100(1). It may then adopt an implementing act designating the country as a “third country posing cybersecurity concerns”.

Before adopting an implementing act under this article, there is no explicit reference or obligation on the Commission to conduct an assessment of the impacts that such an act would have on the Union and whether the cybersecurity risks identified in Article 100(1) outweigh the potential impacts on the Union and its Member States if an implementing act is adopted under Article 100(2).

Similarly, this article does not require explicit Member State involvement or consultation, beyond the final procedure in comitology. More involvement of Member States in the approval process could be achieved through a mechanism similar to the EU Cybersecurity Reserve for the DEP-associated third countries in the Cyber Solidarity Act (Article 19 (3-6)) by means of a Council Implementing Act.

Question 3 - Article 103(4) provides that the Commission shall assess potential risks and dependencies including economic and societal considerations before adopting the implementing acts provided in Article 103(1) and (2), restricting the use of ICT components or components that include ICT components from high-risk suppliers as identified in Article 104. Should a similar assessment of impact be created for the designation of a third country as a country of concern? What other entities/bodies should be involved in the assessment of impact process to capture the full spectrum of risks arising from the potential designation of a third country of concern?

Question 4 - Potential consequences for the designation of a third country posing cybersecurity concerns go beyond that of the designation of high-risk suppliers. In recognition of this, do Member States believe that the proposed text and comitology processes sufficiently engages with them and safeguards their concerns? Would Member States prefer or support a different mechanism to designate third countries as countries posing cybersecurity concerns such as a Council implementing decision?

3) High Risk Suppliers

Background:

Another consideration for the Presidency is how the potential impacts of the use of the ICT Supply Chain will be assessed prior to the deployment of the mechanism. The Presidency understands that this is a key issue for Member States given the wide range of potential impacts deployment of the mechanism could have. The Presidency understands that the risk assessment will analyse the risks that key ICT assets, or a component in key ICT assets in the ICT supply chain, can pose. There is a clear need to analyse the impact that mitigation measures, including banning of ICT components of ICT assets, or ICT assets from high-risk suppliers across the supply chain will have. This is addressed in the current proposal through Article 103(4) where potential social and economic impacts are taken into account by the Commission before adopting implementing acts proposing adequate mitigation measures.

Question 5 - Under Article 22 of the NIS 2 Directive and Article 99 of the proposed Title IV, the NIS Cooperation Group is empowered to conduct the security risk assessment. What other EU entities/bodies, if any, should be involved in the risk assessment process, for designating high risk suppliers, to capture the full spectrum of risks in the ICT supply chain mechanism?

Question 6 - In the current proposal of Title IV, as part of the adoption of the implementing act, the comitology process is used to prohibit use of high-risk suppliers after the security risk assessment carried out as per Article 99 and the economic and societal impacts are assessed by the Commission as per Article 103 (4). Does this process provide sufficient clarity, information and methodology for Member State experts to make a complete judgement during the comitology process?

PUBLIC