Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2026/0011 (COD)

Brussels, 04 September 2026

WK 13545/2026 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:	Presidency
To:	Horizontal Working Party on cyber issues (attachés)
N° Cion doc.:	ST 5611/26 + ADD 1 - 4
Subject:	Cybersecurity Act 2: explanatory note on Title III (European Cybersecurity Certification Framework)

Delegations will find attached an explanatory note from the Presidency regarding the changes which have been introduced in Title III (European Cybersecurity Certification Framework) as set out in WK 11263/26.

Title III European Cybersecurity Certification Framework - Explanatory Note

Introduction

Throughout July and August, the Presidency has worked to produce a REV2 text on Title III on the European Cybersecurity Certification Framework. The Presidency has created this explanatory note during the summer break in order to enhance discussions at the Working Party on 14 September. It should be noted that it is not intended that additional explanatory notes will follow future revisions of the text. This explanatory note will provide a high-level summary of the approach the Presidency has taken to the REV2 text. We have endeavoured to take on board member state views and while we hope that we are closer to achieving a final text on this title, we welcome further engagement with member states on where they feel more work is required.

Cyber Posture

The REV2 text has not introduced changes directly related to cyber posture, and any provisions that directly mention cyber posture have not been altered. This approach was taken due to the request of several MS for further discussion on this topic. The Presidency therefore intends to organise a working party on 10 September, with an agenda item dedicated solely to Cyber Posture. The aim of this session will be to enable MS to engage directly with the Commission and Presidency on this topic before any substantive changes are made to the provisions relating to cyber posture.

European Cybersecurity Certification Group (ECCG)

The Presidency has also chosen not to make any major changes to the structure of the ECCG in the REV2 version of the text. It has been clear from engagements with MS that many wish to see changes to the current way the ECCG operates, however, it must be recognised that the ECCG has its own procedures that it elects through Article 90(8). As a strictly technical advisory body, it currently has no ability to make any decisions in its own capacity. It should also be noted that the ECCG adopts its rules of procedure by simple majority of its members, based on a proposal by, and in agreement with the Commission. Having considered the proposals put forward on the ECCG, it is our view that the degree of flexibility within the ECCG to set their own methods of operation allows for them to adapt and change the way they operate which may not be possible if it hardcoded into legislation. Therefore, to better understand how the member states envisage the role of a reformed ECCG in the request and development process of a certification scheme, the Presidency will issue guiding questions to Member States in late August/early September on this topic. For the time being, the presidency has strengthened the language around the ECCG's opinion and where it is appropriate that it is taken into account.

Interplay of the REV2 text with Other Titles

Some elements of Title III specifically interact with other parts of the text, in particular Title II on the Mandate of ENISA and Title IV on ICT Supply Chain Security. For example, Article

85(9) in Title III relies on Article 102 in Title IV. The Presidency will consider these articles when a REV1 text on Title IV is published in September. Elements that are referenced from Title II such as Article 79(2)(c) on Fees will be discussed in their corresponding articles under Title II, in this example that is Article 46 and 47.

PUBLIC

Summary of Changes

Chapter I: Objectives, Scope and Procedures

Recitals relating to these provisions have been overhauled to emphasise the voluntary nature of certification schemes in recitals 87 and 91 in line with Member State requests to have this stressed in the text. On the European Cybersecurity Certification Assembly, Article 72 introduces more language that will increase transparency on how the Assembly will run procedurally, and how stakeholder input will be utilised, or not, by the Commission. This was included to capture Member State requests for increased transparency around how stakeholder feedback is used in the process. Article 72 also introduces a formalized process for the feasibility study that was requested by Member States. This will be conducted by ENISA and will support the preparation for the planning and development of cybersecurity certification schemes as well as foresee any issues that would delay the schemes' eventual publication This measure will therefore increase the efficiency of the ECCF and the publication of schemes.

The ECCG's role at the initial stage of requesting a scheme is also further clarified in recital 86b. Article 74 has been updated to give more flexibility around the timeline of scheme development, which can be specified in the request itself. This was added to ensure that a timeline is observed for added accountability on their development, but with additional flexibly as Member States have also highlighted that a one size fits all approach may not work in this situation. More language has been introduced to strengthen how ENISA will take the opinion of the ECCG into account when preparing the candidate scheme, and how existing national schemes are taken into account. This article now also further clarifies the process around suspended schemes.

Article 75 is strengthened by Recital 88, which clarifies that the purpose of maintenance is to keep the scheme updated without substantively changing their subject matter, scope or legal effects, in line with comments from Member States. It also further qualifies the process for evaluation, review and withdrawal of schemes taking on board a number of comments from Member States around how this can be made clearer. Article 77 has been updated to reflect common specifications and to take account for the need-to-know basis required for access to data concerning schemes relating to cyber posture. Finally, language has been inserted in Article 79 to ensure the ENISA website includes not only national cybersecurity certification schemes that have been replaced by EU schemes, but also those that are in the process of transitioning. This was added at the request of Member States for more clarity on how national and European Schemes will interact, once a scheme at the EU level is published.

Chapter II: Content of European Cybersecurity Certification Schemes

Based on MS comments, updates were made to the security objectives of European cybersecurity certification schemes in Article 80(1). The Presidency has updated them to include that they ensure entities involved in the lifecycle of the ICT products, ICT services and

ICT processes are sufficiently secure, and to ensure entities prevent or minimise the impact of incidents on recipients of its services and on other services. They also ensure that entities manage the risks posed to these systems used by the entities for their operations or for the provision of their services. On the elements of the schemes themselves in Article 81, minor additions have been made at the request of Member States, such as the inclusion of whether conformity self-assessment is permitted under the scheme, and the provision of information on transitioning from national schemes to European schemes.

Chapter III: Governance for the European Cybersecurity Certification Framework

Language on separation of the supervisory and certification activities has been added to the text through Recital 112 to Article 85(5) on the issuance of European cybersecurity certificates in order to further clarify the degree of separation required. At the request of Member States:

- In Article 86 (3), the text now clarifies that certificates issued under national schemes can be maintained even after the adoption of a European scheme, pursuant to Article 74(9). This will ensure that certified entities are not unduly affected by the transition from national to European schemes.
- In Article 88, the national cybersecurity certification authorities' ability to withdraw certificates is given more flexibility, by empowering them to request the conformity assessment body that issued the certificate to execute the withdrawal when the prior approval model or general delegation apply.
- Additional text has also been added in Article 88 to empower NCCAs to reclaim from a conformity assessment body or holder of a European cybersecurity certificate or issuer of EU statements of conformity the totality of the costs of their activities with respect to instances of failure to cooperate or obstruction of the exercise of the relevant investigatory powers.

On the ECCG, the language on their tasks has been updated in Article 90 to clarify their power to adopt opinions on candidate schemes prepared by ENISA, as well as to advise and assist the Commission in organising the European Cybersecurity Certification Assembly. On challenges with regard to the competence of conformity assessment bodies, language has been included in a revised Article 94 that ensures the Commission will provide any relevant information or findings obtained during the investigation, without prejudice to applicable confidentiality requirements in order to increase transparency as requested by Member States.

PUBLIC