Council of the European Union
General Secretariat

Interinstitutional files:
2026/0011 (COD)

Brussels, 21 September 2026

WK 14493/2026 INIT

LIMITE

CYBER

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 (attachés)
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) - Presidency presentation of Title II amendments

Delegations will find attached a presentation by the Presidency of the amendments introduced in Title II (ENISA) of the second compromise text of the 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). This presentation was made at the meeting of the Horizontal Working Party on Cyber Issues on 21 September 2026.

PUBLIC

Title II: ENISA – REV2

éire2026.eu
ireland2026.eu

21 September 2026

Recap on Title II

PUBLIC

- REV2 text was released on 08 September
- Progressing towards a mature text
- Outstanding Issues - Definitions, Fees, Cyber Liaisons
- MS invited to highlight outstanding issues/red lines

Chapter I: Mission and Objectives

PUBLIC

Mission of ENISA - Article 3

Text added to further clarify ENISA's mission. Art 3(2) adds text outlining how ENISA shall cooperate as appropriate with relevant stakeholders.

Objectives of ENISA – Article 4

New 4a added to reflect role of ENISA – language added concerning ENISA as a centre of expertise

Additional changes made to ensure facilitation of cooperation between ENISA and the CSIRT network and EU-CyCLONe and the relationship between ENISA and ECCC.

Chapter II: Tasks

PUBLIC

Capacity Building – Article 6

Article 6(1)(7) is merged into Article 6(1)(4) to ensure CSIRT cooperation

Recital 16 added to clarify that guidance from ENISA should be more scalable

International Cooperation – Article 9

Text also added to emphasise cooperation with international standards organisations.

New recital 23a added to qualify the nature of ENISA's engagement with international exercises

Chapter II: Tasks

PUBLIC

Operational Cooperation at Union level – Article 10

Article 10(1) – Text altered to more clearly define ENISA's role with respect to the role of MS in operations. Now clarified in Recital 26 - language added that **clarifies that ENISA will not engage in operational activities**.

Article 10 (4) – Text modified to clarify the differing tasks and important contributions of ENISA in the CSIRT and CYCLONE networks.

Shared Cybersecurity Situational Awareness – Article 11

Recital 29 has been partially updated. The repository will be subject to Article 67. Text also amended in 11(1a) to minimise duplication and improve clarify.

Support in incident response and review – Article 13

Article 13(2) language has been added to specify type of incidents ENISA should review and assess.

Cybersecurity exercises at Union Level – Article 14

Article 14(1) Amended to include references to the CSIRT and CYCLONE networks . Recital 38 updated to further clarify how ENISA should complement and support what is being done at a national level with regard to cyber exercises.

Article 14(2) new language added on ENISA role with regard to implementing lessons learned from exercises.

Chapter II: Tasks

PUBLIC

Vulnerability Management Services - Article 16

New Article 16(ba) added to ensure ENISA can provide advisories, corrective or mitigating measures or detection mechanisms related to vulnerabilities on vulnerability management.

Article 16(1)(c) Language introduced to clarify and further specify the aim of structured cooperation with organisations providing similar vulnerability databases. Text reflects the language in Recital 63 of NIS, which is also tied with Article 12 of NIS2.

Standardisation, technical specifications and guidance – Article 18

Article 18(1) – language updated to take account of MS comments on consistency of text

Chapter III: Composition of ENISA

PUBLIC

Article 25 - Composition of the Management Board

Article 25(3) – Text amended to reflect MS desire for appropriate representation on the Management Board

Article 28 – Functions of the Management Board

Article 28 (1)(ma) – Role of Chief Information and Technology Officer legislated for in the text. The role will also be responsible for ENISA's information and data management strategy that shall be adopted by the MB pursuant to Article 28(1)(ha).

Chapter IV: Structure of ENISA's Budget

PUBLIC

Fees - Article 47

PRES understands that several MS have raised issues in their comments. The concept of **exempting public authorities from fees** on the basis that such fees may amount to additional contribution on top of the general budget contributed to by each MS is something that we are considering, and we are aware from our discussion that it raises a significant legal question and would require justification. For the moment, **we have added the exemption in square brackets until more clarity can be provided.**

Changes in Article 47(3) to reflect the fact in exceptional cases where it is justified by substantial additional costs, fees may be levied on public authorities, in relation to testing tools.

Chapter V: Staff and Liaison Officers

PUBLIC

Liaison Officers - Article 58

On the liaison officers, PRES understands the need to ensure such a role is clearly described in the text and provides for a net benefit in being a coordination point between individual MS and ENISA.

We also understand that leaving this as a voluntary measure may not guarantee sufficient representation across the Union and, therefore, we decided to compromise providing for one mandatory liaison officer. In response to MS comments, we have updated recital 72a to make it abundantly clear that a liaison officer is an SNE and there is no difference in their role versus a standard SNE.

Chapter V: Staff and Liaison Officers

PUBLIC

Protection of Personal Data / Security Rules on Data - Article 66 -67

Article 66(1) – In response to Data Protection issue here and generally throughout the CSA 2 proposal.

PRES has taken the opportunity in a new Article 67(2) to clarify the rules that ought to apply and the various information sharing / traffic light protocols that should be observed when ENISA is handling /exchanging info from various sources, including MS and EU entities.

Additionally, PRES has added a new subpar (3) to require the Management Board to adopt an information and data management strategy.

PUBLIC

Míle Buíochas!