Council of the European Union

Brussels, 7 September 2022
(OR. en)

12151/22

LIMITE

CSC 374
CYBER 288
CSCI 129
CIS 88

NOTE

From:	General Secretariat of the Council
To:	Council Security Committee
No. prev. doc.:	7474/22
Subject:	Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union: preparation of the CSC opinion on security of information aspects - Draft opinion

Delegations will find attached a draft opinion on the information security aspects of the proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union[1]. The text was prepared on the basis of the outcome of the discussions held on 8 June and 7 July 2022 as well as the comments received from delegations [2].

Delegations are invited to approve the draft opinion in the Annex by the means of written consultation ending **Wednesday, 14 September, 17h Brussels time**. If no comments are received by then, the draft opinion will be considered approved.

[1] doc. 7474/22 + ADD 1
[2] WK 8691/22 (NL)

ANNEX

DRAFT

Opinion of the Council Security Committee

on security of information aspects of the proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

1. This opinion was requested by the Horizontal Working Party on Cyber Issues on 23 May 2022[3].

2. The Council Security Committee discussed the text of the Commission proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union[4] ("the Cybersecurity Regulation") at its meetings on 8 June[5] and 7 July 2022[6].

3. After a thorough examination of the proposal and in particular the parts relating to or impacting information security and protection of EU classified information, the Council Security Committee (CSC) agreed on XX September 2022 on the following recommendations that form the content of its opinion requested by the Horizontal Working Party on Cyber Issues.

4. The recommendations are structured around three main issues that the CSC has identified:

   A. References to EU classified information (EUCI);

   B. Relation to the Commission proposal for a Regulation on information security in the institutions, bodies, offices and agencies ("the Information Security Regulation").

   C. Obligations to inform, share and notify.

5. For each issue, the opinion presents a rationale and suggests either a way ahead or modifications to be made. Changes to the Commission proposal (doc. 7474/22) are in **bold underlined** for new text and in ~~strikethrough~~ for deleted text.

---

[3] WK 7487/22
[4] doc. 7474/22 + ADD 1
[5] doc. 10136/22
[6] doc. 11228/22

A. References to EU Classified Information (EUCI)

1. Scope of application

It needs to be clarified that the scope of the proposed Regulation does not cover any matter concerning communication and information systems (CIS) or network and information systems (NIS, as used in this Regulation) processing EU classified information ("classified systems).

Only a limited number of Union institutions, bodies and agencies actually run such classified systems which are subject to specific rules, policies and risk management processes. In addition, it would be inappropriate to share widely any operational details and cybersecurity plans of classified systems. Further on, classified systems usually do not fall within the scope of responsibilities of national CERTs.

It is thus recommended to add an explicit exclusion clause that should be added to Article 2. Article 4(2) should also be amended accordingly.

Article 2
Scope

This Regulation applies to the management, governance and control of cybersecurity risks in network and information systems operated by all Union institutions, bodies and agencies for handling unclassified information and to the organisation and operation of CERT-EU and the Interinstitutional Cybersecurity Board.

This Regulation shall not apply to network and information systems handling EU Classified Information (EUCI).

Article 4
Risk management, governance and control

(…)

2. The framework shall cover the entirety of the **unclassified** IT environment of the concerned [..].

2. Incidents in CIS processing EUCI

The Committee supports the possibility that Union institutions, bodies and agencies may consult CERT-EU concerning incidents involving communication and information systems processing EUCI. Article 12(7) already clearly states that it must be explicitly requested by the Union institutions, bodies and agencies operating such classified systems. However, it should be amended to state explicitly that if CERT-EU is consulted for such a case it is at the discretion of the Union institutions, bodies and agencies concerned to define the respective procedure (i.e. when, what and how incident related information is communicated), and that the provisions of Chapter V of the Cybersecurity Regulation do not apply.

Article 12
CERT-EU mission and tasks

(…)

7. CERT-EU may provide assistance to Union institutions, bodies and agencies regarding incidents in classified IT environments if it is explicitly requested to do so by the ~~constituent~~ **Union institutions, bodies and agencies concerned in accordance with their respective procedures. In this case the provisions set out in Articles 19 to 21 of this Regulation shall not apply.**

B. **Relation to the proposed Information Security Regulation**

The Committee is of the opinion that there are overlaps and inconsistencies between this Regulation and the proposed Information Security Regulation, in relation to the respective requirements set by the two texts for securing systems that handle unclassified information. One example that has been identified is the fact that the Cybersecurity Regulation requires multi-factor authentication for the access to all unclassified information (Annex II (2)) where in the Information Security Regulation this is only obligatory for the access to sensitive unclassified information (Article 17 (1(a)). The same issue can be identified concerning the requirement of a "zero trust architecture" (in the Cybersecurity Regulation, Annex II (1), in the Information Security Regulation, Article 17 (1(h)).

Despite the argumentation of the Commission[7] that the two regulations are complementary, the Committee is still concerned that requirements contained in each proposal are not always formulated in the same way and with the same level of detail. In order to avoid inconsistency or ambiguous interpretation and to facilitate their correct implementation, it is important to ensure that both regulations are coherent.

The Committee proposes two options as solutions:

Option 1: Aligning the provisions for CIS handling unclassified information in both regulations, in order to avoid any possible differences in the interpretation of their respective requirements.

Option 2: Moving provisions concerning the security of CIS handling unclassified information (e.g. Article 17) from the Information Security Regulation to the Cybersecurity Regulation, and simply referring to these provisions in the Information Security Regulation.

C. Obligations to inform, share and notify

1. CERT-EU obligation to inform about contacts with national services

While the Committee agrees that CERT-EU should inform the Commission's Security Directorate as the responsible authority about contacts with national security and intelligence services it does not see the need for an obligation to also communicate this always to the chair of the IICB. This should be at the discretion of the responsible authority on a case by case basis. Article 18(5) should be amended accordingly.

[7] WK 10961/22

"Article 18

Information handling

(…)

5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate. ~~and the chair of the IICB~~ without undue delay~~.~~

2. Sharing and notification obligations

The sharing and notification obligations in Articles 19(4) and 20(5) respectively are proposed to neither cover EUCI, nor information received by a Union institutions, bodies and agencies from a Member State Security or Intelligence Service or law enforcement agency.

Regarding the latter, as the national security remains the sole responsibility of each Member State, it would be more appropriate to consider that all information received from the national security actors are excluded from the sharing and notification obligations *unless* this is explicitly allowed by the Member State Security or Intelligence Service or law enforcement agency.

The Articles 19(4) and 20 (5) should be amended accordingly.

"Article 19

Sharing obligations

(…)

4. The sharing obligations shall not extend to EU Classified Information (EUCI) and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency **unless that Member State Security or Intelligence Servive or law enforcement agency explicitly allows this information to be shared with CERT-EU.** ~~under the explicit condition that it will not be shared with CERT-EU.~~

Article 20
Notification obligations

(…)

5. The notification obligations shall not extend to EUCI and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency **unless that Member State Security or Intelligence Servive or law enforcement agency explicitly allows this information to be shared with CERT-EU.**~~under the explicit condition that it will not be shared with CERT-EU.~~