Council of the European Union
General Secretariat

Brussels, 09 June 2022

WK 8402/2022 INIT

LIMITE

CSC
CSCI

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:	Security Committee
N° prev. doc.:	WK 7697/22
N° Cion doc.:	7670/22
Subject:	Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union: revised draft opinion of the Council Security Committee

1. Delegations will find attached a revised draft CSC opinion on the proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union.
2. The draft opinion was modified to take into account the outcome of the CSC discussion on 8 June and the comments received from delegations (WK 7987/22 and WK 8364/22).
3. The main change in Annex I (explanatory part) was made in section III, point 9 where a new paragraph was added to recall the need to strike a right balance, in the specific case of EU institutions, between their autonomy and common security standards for all EU institutions, bodies and agencies.
4. In Annex II (the text of the opinion), changes were made in points 1, 3, 5 and 8, and a new point 6 was added following the request of some delegations to emphasise the possible impact of the future common rules on national rules and legislation.
5. The proposed changes to the initial draft (WK 7697/22) are marked in **bold underline** for new text and in ~~strikethrough~~ for deleted text.
6. Delegations are invited to approve the text in the Annexes I and II by the means of **written consultation** that will end tomorrow, **Friday 10 June, at 17h.** If we do not receive your reaction by then, we will consider the text aas pproved by your delegation.
7. Once the draft opinion is approved, it will be sent to Antici.

ANNEX I

Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union: draft opinion of the Council Security Committee

I. Introduction

1. On 22 March 2022, the Commission adopted a proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union[1] (proposal).

2. On 1 April 2022, the Permanent Representatives Committee approved a mandate[2] for the Council Security Committee (CSC) to prepare an opinion by 15 June 2022. The CSC was asked to provide an initial view on the main aspects of the proposal and any changes to be envisaged as far as the part on the protection of classified information is concerned.

3. **The CSC examined the proposal at its meetings on 26 April and 8 June 2022.**

II. Commission proposal

4. On 26 April 2022, the Commission presented its proposal to the CSC. The Commission stated that the aim of the initiative was to address the current situation characterised by EU institutions, bodies, offices and agencies having either their own information security rules, or not having any such rules at all in a context where these organisations handle an increased amount of classified and sensitive non-classified information. In addition, the Commission had observed a great diversity of practice in the area of non-classified information. According to the Commission, the fragmentation of the legal frameworks and disparate practices hamper sharing of information across EU institutions, bodies, offices and agencies and lead to under-classification or non-classification, which in turn exposes information handled by the EU administration to evolving cyber and hybrid threats.

[1] 7670/22 + Annexes 1-8.
[2] 7676/22

5. To remedy this situation and in line with the conclusions reached by the European Court of Auditors in its special report on the cybersecurity of EU institutions, bodies, offices and agencies[3], the Commission proposes to establish a single set of information security rules that would be common to all EU institutions, bodies, offices and agencies. In parallel the Commission has also prepared a proposal on high common standards on cybersecurity at the institutions, bodies, offices and agencies of the Union[4].

6. The proposal aims to cover all information handled by the EU administration, whether non-classified or classified. The Commission stated that the proposal is based on a risk-management approach and respect the autonomy of each organisation.

7. Another main objective of the initiative is to reinforce cooperation between EU institutions, bodies, offices and agencies. The Commission proposes that this be done via the establishment of a permanent governance structure to which the Commission would provide secretariat or another form of support.

8. Finally, the proposal aims to modernise the information security rules in line with the digital transformation and the expansion of teleworking.

III. General exchange of views within the CSC

~~At the meeting on 26 April 2022, delegations were invited to share their initial general views on the proposal, focusing on the main issues and their most important concerns.~~

9. While delegations in general welcomed the Commission initiative, they identified key parts of the proposal that need**ed** to be substantially and structurally modified in order for the initiative to reach its aim of creating uniform and strong rules for the protection of EU classified information (EUCI) across all parts of the EU administration. The areas concerned ~~are~~ **were** the following:

[3] Special Report Nr 05/2022 entitled "Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats" (doc. 8040/22)
[4] 7474/22

a. Given the fact that the protection of EUCI is also part of national security, delegations consider that the proposal does have an impact on national laws and regulations, such as those related to industrial security, cryptographic products or personnel clearance processes. The proposed governance which gives Member States only an advisory function is not satisfactory in their views and should better reflect the leading role of Member States in certain areas of information security.
b. The proposed governance is unclear regarding the roles to be exercised by different stakeholders. In this regard, it needs to be clarified how the establishment of the Interinstitutional Information Security Coordination Group will affect the functioning of the Council Security Committee and other information security-related groups across the EU administration.
c. Regarding the inclusion of non-classified information together with classified information in the same legislative text, delegations see a risk of creating undesirable consequences on EUCI protection standards, in particular for information classified RESTREINT UE/EU RESTRICTED that in practice could be replaced by sensitive non-classified information.
d. <u>While in the specific case of EU institutions, their autonomy to decide on their internal organisation should be respected, the common setting of security standards defined for all EU institutions, bodies, offices and agencies should be ensured.</u>

IV. Opinion

~~On the basis of the outcome of the discussion held at the CSC meeting on 26 April and the comments made, delegations can find in the <u>Annex</u> to this note a draft CSC opinion on the proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union. Delegations are invited to examine the text of the draft opinion contained in the Annex to this note at the CSC meeting on 8 June.~~

10. <u>On … June 2022, the CSC approved, by means of written consultation, the opinion that can be found in the Annex to this note. The opinion brings to the attention of Antici a set of major issues that the CSC deem necessary to be addressed during the detailed examination of the Commission proposal.</u>

ANNEX II

DRAFT

Opinion of the Council Security Committee
on the proposal for a Regulation on information security
in the institutions, bodies, offices and agencies of the Union

On the basis of the mandate received from the Permanent Representatives Committee[5], the Council Security Committee has prepared this opinion on the main aspects of the proposal and changes to be envisaged. The opinion focuses mainly on the part concerning the protection of EU classified information (EUCI). It also mentions certain provisions dealing with non-classified information, in particular in situations where the inclusion of this category of information in the same proposal may have an impact on the protection of EUCI.

The Council Security Committee welcomes the Commission proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union[6] ('the proposal'). It agrees there is a need to identify the protection of information as one of the most important areas of improvement for the European Union.

It is nevertheless the Committee's view that the proposal will need to be substantially and structurally modified in order for the regulation to reach ~~its~~ **the** aim of creating uniform and strong rules for the protection of EUCI across all parts of the EU administration, while respecting the autonomy of each Union institution to decide on its internal organisation.

[5] 7676/22
[6] 7670/22

The Council Security Committee has identified the following issues that will need to be addressed further during the detailed examination of the text:

1. The proposed legal basis, Article 298 of the Treaty on the Functioning of the European Union (TFEU), allows for the adoption of measures of a supporting nature with regard to EU institutions. **In the specific case of EU institutions, s**uch measures should respect the**ir** ~~institutions'~~ autonomy and **should** not interfere with their 'power of internal organisation'. A detailed analysis of each provision will be necessary to ensure that they respect the limits of the chosen legal basis.

2. The binding common rules contained in the proposal are to be implemented in each organisation through its own internal implementing rules and policies that will be designed and decided by the security authority of that organisation. It will be therefore important, during the detailed examination of the text, to pay attention to the level of detail to be kept in the common rules knowing that only such rules should be directly applicable to the EU administration, while the rest should be left to the discretion of each organisation's security authority as long as it would be in line with the Regulation.

3. The draft Regulation as proposed by the Commission would establish a new interinstitutional governance led by an Interinstitutional Information Security Coordination Group that would bring together the security authorities of all EU institutions, offices, bodies and agencies and would be mandated to define common policy in information security for all parts of the EU administration. The Coordination Group would not have any decision-making powers, **but would be rather drawing on the experienced-based advice of its members**. **F**urther reflection will be needed to understand how it is supposed to interact with the governance mechanisms that currently exist in the EU.

4. In this regard, it is particularly important to ensure that the future rules are without prejudice to the role and prerogatives of the Council under the Treaties. Concerns were mainly raised regarding two elements of the proposal: firstly external relations, where the Council's role in international agreements is not fully reflected (Article 55 of the proposal only refers to Article 218 TFEU). In addition, it remains unclear whether and how the Council's powers regarding implementing arrangements and assessment visits would be impacted. Secondly, in the area of the cryptographic products, the level of obligations remains weak. The references made to in Article 42 of the proposal to the Council's list of approved crypto products is not sufficient to ensure that the current process for the approval of crypto products, including second-party evaluation, will be preserved.

5. In addition, Member States have extensive knowledge and experience in other crucial areas of the protection of EUCI, such as personnel security, TEMPEST approval and industrial security. While the scope of proposal is limited to the EU administration, Member States would be given an advisory role in the proposed security governance through their participation in an information security committee. ~~Further reflection will be, however, needed to understand whether this mechanism~~ **The current proposal might not** sufficiently take into account Member States' ~~crucial contribution to~~ **unique position regarding** the protection of EUCI **in line with Article 4(2) TEU and will therefore need further reflection.**

6. Furthermore, given the fact that the protection of EUCI is not only required to protect the interests of the Union, but also of its Member States, further assessment of the impact, both direct and indirect, of the proposal on national laws and regulations, in particular those related to industrial security, cryptographic products or personnel clearance processes, will be needed.

7. The Council Security Rules were historically the first security rules established within the EU administration with the aim to protect EUCI. They have been gradually complemented by security policies and guidelines, which together create a comprehensive and solid framework for the protection of EUCI that serve as a guide for other EU entities when they want to establish or modernise their own rules pursuant to the *'Common approach on sharing EU classified information with EU institutions, agencies, offices and bodies'*[7]. The 2013 Council Security Rules are currently under review in order to be simplified, modernised and made more efficient to deal with the current threat landscape. It would therefore be important, when examining the proposal, to take into due account the provisions agreed by the Council Security Committee during the review process (physical security, relations with third States and international organisations, and management of classified information) in full compliance with Article 298 TFEU.

8. Finally, the inclusion of non-classified information together with EUCI in the same text may have ~~potential~~ negative consequences~~, however unintentional,~~ on the protection standards for EUCI. Such provisions could lead to a confusion between the protection rules on sensitive non-classified information and information classified RESTREINT UE/EU RESTRICTED. Further analysis will be needed on the **possibility** ~~benefits and disadvantages~~ of having **two** ~~one~~ instrument**s**, **one** for ~~both~~ classified and **one for** non-classified information.

[7] 6074/17