Council of the
European Union

Brussels, 16 December 2022
(OR. en)

16162/22

LIMITE

CSCI 204
CSC 595
CSC-TSCM 3

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Outcome of proceedings of the Council Security Committee (Information Assurance) meeting held on 16 November 2022

1. Adoption of the agenda

The agenda as set out in CM 5124/2/22 REV 2 was adopted with additional point under AOB on the outcome of the ARG meeting that took place on 16 November 2022.

2. Review of the Council Security Rules: CIS Chapter

The Chair informed delegates about the view of the Council Security Committee to use the revised Council Security Rules as "blueprint" for the Information Security Regulation examination. Discussions on the revision of the CIS chapter were based on the WK 14870/2022 REV 1. The Chair went through each revised article and collected the delegations' comments who welcomed the proposed approach and the respective changes. In particular delegations supported the idea of flattening the CSR by combining provisions from Article 10, Annex IV and some policies and guidelines as well as moving some generic definitions and principles to the General Provisions Chapter.

In the area of accreditation, the period of maximum 3 years validity of the accreditation statement was discussed, where most of the delegations who took the floor supported this time limit, while others considered it too short due to the workload involved and suggested different periods for the different levels of classification. Delegations stressed that the accreditation should be based on compliance with the security rules and risk management process. With respect to the use of Interim Approval To Operate Member States expressed the view that it should clearly mention the conditions under which it was granted and its renewal possibilities should be limited.

In the area of TEMPEST protection delegations pointed out that the Council Security Rules should not allow deviation from the TEMPEST selection and installation requirements for EUCI classified S-UE/EU-S and above. Furthermore, with respect to the distribution of tasks and functions of the CIS security authorities delegations expressed the need to clarify the conflict of interest between different functions being accumulated in the same authorities and proposed appropriate segregation of duties.

In the area of secure interconnection of CIS delegations expressed support for the proposal of setting out a requirement to have a business reason to interconnect, as opposed to a technical facility and suggested to phrase it as a positive one.

For what concerns the electronic storage media requirements, delegations suggested to move it in the management chapter of the CSR. Finally, in the area of emergency circumstances delegations proposed to add a requirement on clarifying and reporting the circumstances that lead to an emergency situation.

Given the fact that some of the proposals were having an impact on the General Provisions and Definitions Chapter of the CSR the Chair informed delegations that would report to the CSC and ask for its approval of the approach or further guidance on how to proceed.

Delegations were invited to send written comments by the end of November 2022. Member States challenged this date as being too short due to the complexity of the text. The deadline was extended by the end of the year, nevertheless GSC asked for constructive comments before the CSC meting to be held on 7 and 8 December 2022.

3. Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union – Chapter 3 & Section 5

Following the mandate received from the CSC, the CSC-IA examined Chapter 3 and Section 5 of the proposed Information Security Regulation. During the article-by-article examination delegations questioned the lack of provisions for CIS handling 'normal' information and requested to add a reference to the five security principles (confidentiality, integrity, availability, authenticity and non-repudiation) set out in Article 4. They also criticised the foreseen governance concept, expressing concerns about being excluded from the development and approval of policies and insisting that the same rules should apply whenever EUCI was handled in CIS. They were seriously concerned that through the non-binding implementing rules regulation would allow different levels of security throughout the EU while handling and storing Member States' national classified information transmitted to the EUIBAs. Delegations also requested a number of clarifications to the text mainly regarding the functions of the foreseen bodies, stressing the need to avoid conflict of interest whenever one entity was fulfilling more than one function.

Several delegations called for foreseeing a reporting obligation of the security weaknesses and incidents to the Member States. A number of delegations raised concerns regarding the provisions on cryptographic products approval defining them as inappropriate and unrealistic since interfering with Member States' national competencies. Furthermore, delegations underlined the lack of mention in the regulation of the possibility to use unencrypted distribution systems and criticised the extension of the requirement on using cryptographic products on the storage of EUCI which was not in line with the CSR.

Delegations also expressed doubts regarding the possibility the Security Accreditation Authority to perform all required tasks due to a potential lack of expertise in the field of auditing and inspection as well as due to potential conflict of interest (the SAA should not validate its own work).

Finally, delegations assessed that the Crypto Approval Authority could not play any role in emergency circumstances as decisions in this context should be taken by the 'competent authorities'.

Member States were invited to provide comments on the examined articles by 15 January 2023.

4. AOB

The ARG Chair reported the outcome of the ARG meeting of 15 November 2022, explaining in particular the impact of the withdrawal of the approval of a cryptographic product. One delegation raised their concerns and difficulties stemming from the withdrawal and asked for support in finding an appropriate solution.

Further, the ARG Chair informed about the intention to organise a workshop on issues of second party evaluation and approval of cryptographic products in 2023.

The next CSC(IA) meeting was scheduled for 29 March 2023.