Council of the
European Union

Brussels, 22 June 2022
(OR. en)

10136/22

LIMITE

CSC 252
CYBER 214
CSCI 94

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Outcome of proceedings of the Council Security Committee meeting held on 8 June 2022

1. Adoption of the agenda

The agenda as set out in CM 2976/1/22 REV 1 was adopted with the following items added by the Council Secretariat under the agenda item 6:

a) New guidelines on EU crypto material and COMSEC items management

b) COMSEC training held on 11 - 13 May 2022 and EU TEMPEST seminar to be held on 12 - 13 October 2022

c) Full accreditation of the EDA system for level SECRET UE/EU SECRET

The Chair informed the Committee that on 7 June he attended the meeting of the Working Party on Space to present the opinion of the Security Committee concerning the Union Secure Connectivity Programme (doc. 9558/22). The Chair said that the opinion was received positively by the delegates of the WP on Space and that the Presidency of the WP on Space accepted all the recommendations contained in the Committee's opinion and integrated them in a new compromise text (doc. 9654/22).

2. 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: opinion of the Council Security Committee

The Committee examined the draft opinion contained in WK 7697/22. Delegations in general welcomed the draft text including the comments received from the Netherlands delegation (WK 7987/22). The suggestion of the Netherlands delegation to reflect on the possibility to split the instrument in two separate parts, one for classified and one for non-classified information, was in particular supported by some delegations.

One delegation, supported by several others, raised two additional points to be reflected in the opinion. Firstly, it suggested that the text should strike a right balance between the respect for the autonomy of each organisation and the need for common security standards to be applied to all the European administration. Secondly, it asked to include in the text of the opinion an issue mentioned in the introductory part of the opinion that concerns the (indirect) impact of the future Regulation on Member States' national laws and regulation.

The Chair agreed to take both issues on board, while highlighting that the "power of internal organisation" is recognised by the Treaties only for EU institutions.

While some delegations wanted the text to be more detailed on certain points, such as the ways the Committee's functioning might be affected by the proposed governance, others were in favour of more general provisions at this stage. They supported the Chair's view that the aim of the opinion is to bring to the attention of Antici certain major issues which will be need to be addressed later on during the detailed examination of the text.

The Chair concluded that a revised version of the draft opinion that will integrate suggestions raised by the delegations during the meeting will be circulate shortly. He drew the attention of delegations to the fact that since the opinion had to be delivered by 15 June, as per the original request, delegations would have to approve the text by the means of written consultation on a very short notice.

3. Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

The Chair informed the Committee that he had received the letter from Chair of the Horizontal Working Party on Cyber Issues (WK 7487/22) in which the Committee was asked to provide an opinion on the proposal for a Regulation concerning laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (doc. 7474/22). The Chair underlined that the opinion was requested on the aspects of the proposal related to information security and it should be delivered by 15 September 2022.

The Commission presented its proposal with a particular focus on information security-related aspects (WK 8370/22). It recalled the proposal's objectives which is to establish common cybersecurity rules and measures for all European institutions, bodies and agencies, improve their resilience and incident response capabilities, and to reinforce the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU). In relation to the provisions dealing with information security, the Commission explained that CERT-EU already provides assistance regarding incidents in classified IT systems if the EU administration requests so explicitly (in line with Article 12 of the proposal), that CERT-EU, as a future inter-institutional Union body, will need to comply with the future regulation on information security when handling classified and non-classified information (Article 18) and that EUCI is exempted from the sharing and notification obligations that Union institutions, bodies and agencies have towards CERT-EU (Articles 19 and 20 respectively).

During the initial exchange of views, delegations raised a number of comments. They found it unclear whether the entire text applies to EUCI and asked for it to be clarified. Regarding a potential assistance of CERT-EU for incidents in classified IT systems, some delegations suggested to reflect on the need to include also the consent of originator of the EUCI concerned before such an assistance is requested. Others wanted to know why the exemptions from the sharing and notification obligations of non-classified information are limited only to information from the State Security or Intelligence Services, or law enforcement agencies. Delegations also expressed doubts about the obligation to inform the Commission Security Directorate about the contacts between national security/intelligence agencies and CERT-EU which could be counter-productive (Article 18(5)). Finally delegations had questions regarding the real capacity of CERT-EU to handle EUCI and operate classified IT systems.

Regarding the scope of the proposal, the Commission said that it did not see the need for more general explicit exceptions for classified information, given that most of the articles of the proposed regulation do not concern information as such at all. The Commission mentioned the role of system owners in the Union institutions, bodies and agencies, who have the responsibility to ensure the security of their systems, regardless of the type of information processed by those systems.

The Commission confirmed that CERT-EU could already provide assistance to the EU administration regarding IT systems which handle EUCI and if CERT-EU was to handle EUCI would have to follow all applicable rules, e.g. the future common rules on information security. Regarding the question why the exemptions from the sharing and notification obligations are not proposed to be wider, the Commission explained that such exemptions must be limited as they go against the overarching principle of knowledge sharing. According to the Commission such situations will arise only in exceptional cases.

The Chair invited delegations to send their written comments by 15 June. A further discussion will be held at the next Committee's meeting.

4*. Review of the Council Security Rules:

a) Industrial security

The Committee held a discussion on the outstanding issues set out in WK 6556/22.

Delegations agreed that the list of requirements proposed by the German delegation[1] would be the basis for the first draft proposal concerning provisions on minimum requirements that NSAs/DSAs shall assess before issuing Facility Security Clearances (FSC). Delegations discussed some of the proposed requirements, in particular those concerning assessment of the ownership or financial control by entities from non-EU countries. Additionally, some delegations suggested minor editorial changes in the text setting out the requirements which the Council Secretariat will take into consideration in the first draft.

Regarding the definition of 'relevant security aspects' related to the preparation of a security classification guide, delegations agreed to use the practical classification guide[2] as the general basis that will be fine-tuned and tailored in the Programme security instructions (PSI) or in other specific arrangements.

Furthermore, delegations discussed the possibility of directly arranged visit in connection with classified contracts. Member States agreed that visits involving access to information classified RESTREINT UE/EU RESTRICTED would be arranged directly between the sending and receiving entity.

With regard to directly arranged visits involving access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, the Council Secretariat noted general support of delegations. Specific conditions that would allow for such visits will be set out in the first draft proposal. One Member State expressed a reservation on possible direct visits within contracts classified at higher levels because of a potential conflict with its national laws and regulations.

The Chair invited delegations that would like to provide comments by writing, to do so by the end of June.

[1] WK 6556/22, paragraph 3
[2] Annex I to the policy on creating EU classified information (doc. 19872/11).

b) Management of classified information

The Committee examined a revised draft of the reviewed provisions on the management of classified information as set out in WK 6863/22, namely Articles 9 to 9e.

On the subject of abbreviated security classification markings, one delegation objected to the proposal to allow abbreviations to replace full security classification markings (Article 9b(2)) because only the latter markings are legally valid. It proposed to restore the text concerning this issue as it stands in the current Council Security Rules.

During an exchange of views on the marking of a security classification level on EUCI, the Commission asked for clarification regarding the marking of electronic media that are used for storing multiple copies of EUCI. This matter will be clarified in a separate paragraph.

The Committee also discussed a proposal of the GSC's Classified Information Office to introduce a stricter provision concerning the registration of copies of EUCI classified at the level SECRET UE/EU SECRET. Such a provision would require a responsible registry to inform the originator's registry about the number of copied, distributed or consulted EUCI. However, delegations were of the view that this could create heavy administrative burden.

One delegation proposed to exclude from the Council Security Rules a possibility to make copies of EUCI at the level TRÈS SECRET UE/EU TOP SECRET, but their suggestion did not receive support of the Committee. This means that EUCI at the level TRÈS SECRET UE/EU TOP SECRET may be copied and translated only with a prior consent of the originator.

The Committee will continue the examination of the text at its meeting on 7 July.

5. EUCI compromise report 2021

The Council Secretariat presented a report describing incidents concerning EUCI in 2021 (WK 6861/22 (RESTREINT UE/EU RESTRICTED)). Overall, delegations welcomed the report and its detailed content.

6. Any other business

a) New guidelines on EU crypto material and COMSEC items management

The Council Secretariat informed delegations that guidelines on EU crypto material and COMSEC items were approved by the Security Committee by means of written consultation on 27 May 2022. The Information Assurance Security Guidelines on the management of EU crypto material and COMSEC items are available in doc. 9729/22 RESTREINT UE/EU RESTRICTED.

b) COMSEC training on 11 - 13 May 2022 and EU TEMPEST seminar to be held on 12 - 13 October 2022

The Council Secretariat informed delegations about the COMSEC training held on 11 - 13 May 2022 in Brussels. The training was attended by more than 70 participants from Member States and Union institutions, bodies and agencies.

Delegations were also informed that the next EU TEMPEST Seminar will be hosted by the Czech Presidency on 12 - 13 October 2022 in Prague.

c) Full accreditation of the EDA system for level SECRET UE/EU SECRET

The Council Secretariat informed delegations that the Council’s Security Accreditation Board has granted an accreditation at the classification level SECRET UE/EU SECRET to the European Defence Agency's system EDA-S.

* Representatives of EDA, EUAA, Europol, Frontex and SatCen were invited to attend the discussion on this item (doc. 9073/22).