Council of the European Union

Brussels, 24 July 2023
(OR. en)

11683/23

LIMITE

CSC 354
ESPACE 37
USA 46

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Outcome of proceedings of the Council Security Committee meeting held on 4-5 July 2023

1. Adoption of the agenda

The agenda was adopted as set out in CM 3272/1/23 REV 1.

2.* Review of the Council Security Rules

a) Personnel security: revised draft proposal

The Committee examined the revised draft proposal contained in 10797/23.

The Committee discussed in particular the following issues:

– the scope of Article 7ba on potential access to EUCI. It was agreed that the article will be split to address, on the one hand, couriers who will be required to have a personnel security clearance (PSC) at the appropriate level (CONFIDENTIEL UE/EU CONFIDENTIAL and above), and on the other hand other job categories where security checks will be required as a minimum;

– the security vetting criteria (Article 7d, paragraphs 2 and 3). Since all security vetting criteria were divided in the text between ‘criteria’ in paragraph 2 and ‘elements’ in paragraph 3, one delegation raised a concern that, under its national law, such differentiation could give rise to appeals if the outcome of security vetting was based only on ‘elements’. To achieve an equal level of obligation and weight for both sets of criteria, the GSC proposed to delete the reference to ‘elements’ in paragraph 3. Furthermore, one delegation pointed out that the vetting criterion regarding individuals’ medical background was very sensitive, therefore, the wording should be more generic and should be moved to paragraph 3;

– the wording in Article 7g on authorisation for access to EUCI in the GSC, and in particular its paragraph 3 concerning the information that the GSC needs to receive from NSAs in order to decide whether or not to issue such an authorisation. One delegation was of the view that NSAs should notify the GSC of the PSC, while other delegations were in favour of keeping the current text, which they found well-balanced and suited to the needs of the GSC procedure; the current text requires NSAs to communicate to the GSC an assurance resulting, or not resulting, from the security vetting. One delegation also wanted to further specify the wording on procedures in the GSC following the absence of an assurance from NSAs;

– the obligation of GSC staff to notify the GSC of any significant changes in their personal circumstances (Article 7g, paragraph 11). In general, delegations expressed support for this new obligation, while suggesting that the GSC should inform the responsible NSA when such a notification is made;

– ad-hoc authorisations (Article 7l). The GSC presented a revised text of the article, which aims at making the conditions for issuing this type of authorisations stricter and the process more transparent, with NSAs being informed throughout the whole process. In response to Member States’ comments, in particular on the permitted duration of the recourse to ad-hoc authorisations (paragraph 3), the Chair suggested reducing this from one year to six months, and specifying that the six-month period would begin on the date on which the first authorisation is issued. LU and ES entered a reservation on Article 7l.

b) Industrial security: revised draft proposal

The Committee examined the list of definitions related to industrial security and Articles 11 to 11c of the revised draft proposal, as set out in 10798/23. The Committee discussed in particular the definition of a facility security clearance. Based on Member States' comments at the meeting, the GSC will prepare a new revised draft for the Committee's examination at the next CSC meeting.

c) CIS chapter: draft proposal

The GSC presented the draft text on CIS security as developed by the CSC(IA), as set out in 10799/23. There was broad support for the main changes, with only a few editorial clarifications being suggested and/or requested. The only open issue, the validity of CIS accreditation for a maximum of three or five years, seems to have been resolved, with general support for five years as the common minimum standard. One delegation expressed a reservation on the issue, pending internal consultations.

3. Interim approval of a cryptographic product (R-UE/EU-R)

The Committee endorsed the recommendation to give interim approval for a cryptographic product as set out in 11026/1/23 REV 1 (R-UE/EU-R).

4. 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: governance

The Council Legal Service explained legal aspects related to the possible impact of the proposed Regulation, following written questions and comments from several delegations. The Council Legal Service clarified certain legal aspects in particular related to the scope and possible impact of the proposed Regulation, following written questions and comments from several delegations. The Council Legal Service recalled the Court of Justice jurisprudence according to which, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with EU law.

Following questions from several delegations, the Council Legal Service also highlighted the relationship between the entry into force of the Infosec Regulation and the Council Security Rules and the intergovernmental agreement. The delegations concerned thanked the Legal Service for its explanations, while expressing the view that given these limitations, they maintained a reservation on the initiative while accepting to discuss the text.

The Chair stated that the GSC had tried to take the Member States' comments as far as possible into account in the revised version, as set out in 8453/1/23 REV 1. The composition of the Interinstitutional Information Security Coordination Group (IISCG) had been modified to include only institutions and bodies. Other EUIBAs would be represented by three representatives of the EUAN network. The European Council and the Council of the European Union would have one seat each.

The Chair also confirmed that the concept of 'guidance' in the context of the proposal would not give any binding effect to the recommendations of the IISCG vis-à-vis the EUIBAs and Member States. Such guidance was intended to offer support in particular to the smaller EUIBAs; each EUIBA would however still be able to have its own internal rules, although they would have to be aligned to the common baseline to be defined by the Regulation.

The Chair also pointed out that it was still to be determined in further meetings whether paragraph 3 of Article 8 should be moved to the CIS part of the Regulation, since it was mainly related to that area.

The Council Security Committee reached an agreement on a draft version of Articles 6 to 8, with a general reservation from a few Member States. A new revised text will be presented at the next meeting. The Security Committee also agreed to start discussing non-EUCI at the next meeting in September.

5. Agreement between the European Space Agency and the European Union on the security and exchange of classified information

The EEAS presented the state of play on negotiations to amend the Agreement between the European Space Agency and the European Union on the security and exchange of classified information (security of information agreement) as set out in 11066/23.

The Committee, which is the special committee within the meaning of Article 218(4) TFEU[1], was consulted on the outstanding issue concerning the provision of classified information to contractors (Article 7(5)). The Committee endorsed the compromise, suggested by the EU, that maintains the principle of originator's consent, while addressing the concerns expressed by the European Space Agency regarding the potential administrative burden that this could represent.

Furthermore, the Committee endorsed a proposal raised by one delegation to simplify the wording in Article 10, paragraph 2, which would read as follows: 'If required for specific operational reasons, correspondence from one party, including in electronic form, may be directly addressed to the other party. The related procedures shall be described in the Implementing Arrangement.'

The EEAS will send the text thus amended to the ESA for final approval.

6. Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union of an agreement with the United States laying down security procedures for the launch of Galileo satellites from United States' territory

The Commission presented the recommendation contained in 11233/23 and the negotiating directives set out in 11233/23 ADD 1 REV 1. The Commission informed the Committee that the agreement is needed in order to provide for security requirements that cannot be covered by the contract that will be signed with a US company for the purpose of the Galileo satellite launch. Those security requirements relate to US customs controls, the investigation of security incidents linked to the launch and the recovery of EUCI in the event of launch failures. The Commission concluded by saying that it planned to launch the Galileo satellites in February 2024.

The exchange of views was classified at the level of RESTREINT UE/EU RESTRICTED.

Delegations can send written comments by **11 August 2023**. On the basis of those comments, the GSC will prepare a revised text of the Council Decision which is planned to be discussed at an ad-hoc meeting on **7 September 2023**.

[1] 11576/22.

7. Exchange of classified information with third states and international organisations

The EEAS informed the Committee about Moldova's request to receive EUCI at the level RESTREINT UE/EU RESTRICTED in electronic form, more specifically on offline digital media. In such a case, an additional arrangement between the EU and Moldova would be needed as no electronic release is allowed under the current EU-Moldova Security of Information Agreement and related Implementing Arrangements.

Before formulating its opinion, the Committee asked the EEAS to provide more details on the need for Moldova to receive EUCI in electronic format, as well the updated risk assessment of the situation in Moldova.

8. Any other business

a) Update on activities of the CSC sub-committees

A representative of the GSC briefed the delegations on the meetings of the CSC sub-committees which took place respectively on 15 June (ITTF), 16 June (CSC-TSCM), 20 June (ARG), 21 June (CSC-IA) and 22 June **(**SAB**)**.

b) Protecting the European Council and the Council against terrorism and public order threats

A representative of the Safety and Security Directorate of the GSC gave a presentation of the measures taken by the GSC against terrorism and public order threats.

c) 2023 EU COMSEC training

A representative of the GSC briefed the delegations on the EU COMSEC training event which took place on 30 and 31 May 2023 in Brussels at the GSC premises.

---

* Representatives of the EUAA, eu-LISA, Europol and SatCen were invited to attend the discussion on this item (10727/23).