Council of the European Union

Brussels, 27 April 2023
(OR. en)

8453/23

LIMITE

CSC 187

PUBLIC

Interinstitutional File: 2022/0084 (COD)

NOTE

From:	General Secretariat of the Council
To:	Security Committee
Subject:	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 - Discussion paper on the main issues regarding governance

Delegations will find attached:

- a discussion paper aimed to structure the discussion on the question of governance in the context of the draft Regulation on Information Security in the EUIBAs (Annex I),
- a first proposal for a possible redraft of Articles 6, 7 and 8 of the draft Regulation (Annex II). New text is indicated in **bold** and deletions in ~~strikethrough~~.

These issues will be discussed at the CSC meeting on 4 May 2023.

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

Discussion paper on the main issues regarding governance

I. Introduction

1. The question of the governance structure in the proposal for a Regulation on information security in the institutions, bodies and agencies of the EU was discussed at the meeting of the Council Security Committee on 14-15 March 2023. As a result of those discussions, delegations considered it a priority and agreed to start working on concrete proposals, with a view to strengthening the role of Member States and ensuring an effective mechanism to implement the Regulation, including through guidance documents.

2. The aim of this note is to initiate a first exchange of views on these questions.

II. Main issues

3. The proposed Regulation entrusts the governance to an Interinstitutional Information Security Coordination Group (IISCG) supported by thematic subgroups, a permanent secretariat and an Information Security Committee. It also sets general rules for the organisation of security in each EUIBA.

4. For each of these elements, various issues have been identified, for which corresponding possible solutions are proposed.

A. The Interinstitutional Information Security Coordination Group (IISCG) – Article 6

5. The current proposal with only one meeting a year and all EUIBAs being represented without voting rules risks to undermine the proper functioning of the IISCG.

6. Another difficulty lies in the absence of recognition of the specific role some institutions and bodies play in information security matters, especially regarding the protection of EUCI.

7. In this regard, the Council should be given additional prerogatives, given its competences, the specificities of its work and functioning, not only in political terms but also in particular for instance in the area of protection of EUCI.

8. As a Union's institution within the meaning of Article 13(1) TEU, the European Council should be given a seat in the IISCG.

9. To address these issues, it is proposed:

- to have more meetings of the IISCG per year (3);
- to limit the participation to the IISCG to a specific list which would include all the institutions and a limited number of a few relevant bodies and agencies. All other agencies would be represented by representatives of the Union Agencies Network (EUAN) and may be invited on a case-by-case basis;
- that the chairmanship be entrusted to a common structure composed of the representatives of the European Parliament, the Council and the Commission, each of them holding the chairmanship for 2 years on a rotating basis while the two others would be vice-chairpersons during the given period;
- to maintain the principle of decisions taken by consensus;
- to specify that each represented institution or body should designate a member and an alternate;
- to provide explicitly for the possibility to adopt decisions under written procedure.

B. The Information Security Committee (ISC) – Article 6(8)

10. The Information Security Committee gives a possibility to Member States to provide advice to the IISCG. In order to strengthen this role, it is proposed that:

- it is chaired by a representative of the Council;
- its secretariat is provided by the Council[1];
- the EP, the Commission and the EEAS are always invited, while the chairperson may invite any other EUIBA on a case-by-case basis; and
- it is mandatory for the IISCG [and thematic subgroups] to consult the ISC on any guidance document the implementation of which could have an impact on the Member States or require their contribution.

Such amendments would also make it easier for the CSC to articulate its works with those of the ISC.[2]

C. The thematic subgroups – Article 7

11. The scope of the thematic subgroups as envisaged in the proposal should be clarified. Unclassified information (NCI) is currently covered by two different subgroups: a) the subgroup on non-classified information and b) the subgroup on Information Assurance when it comes to CISs handling unclassified information.

12. An option, put forward by a delegation, would be to establish two completely separate governance mechanisms for NCI and EUCI, i.e. an IISCG-NCI for non-classified information, and an IISCG-EUCI for classified information. This could, however, create additional administrative burden and would raise the question of the role the ISC would play for the IISCG-NCI. Another possibility would be to maintain a single IISCG, but to entrust all questions regarding NCI, including those on the information assurance of CIS handling NCI, to a single new subgroup on NCI.

---

[1] According to the Commission's explanatory memorandum one permanent AD and AST would be needed for the permanent secretariat function within the Commission. The possible budgetary implications in terms of staffing requirements should be taken into account by the Member States themselves in the context of the budgetary planning for the GSC, and also in the context of the next MFF exercise after 2027.

[2] With a chairperson from the Council, it would be for example easier to have meetings of the ISC in the Council, next to CSC meetings. A permanent secretariat by the Council would facilitate the information of the Member States on any development relevant to them.

13. Another issue concerns the composition and functioning of the thematic subgroups. Except for the permanent secretariat to be provided by the Commission, the proposed Regulation is not very specific on these issues, considering maybe that they will be addressed in the terms of reference to be adopted by the IISCG, when not addressed in specific articles of the Regulation. It may however be useful to set some common rules, including regarding the composition, which should be limited in order to keep them manageable.

14. A third issue relates to the interaction of the subgroups with the IISCG and the Information Security Committee. It is proposed to clarify that only the IISCG can adopt guidance documents, but that it may receive recommendations for such documents from the thematic subgroups. Regarding the ISC, a possibility for consultation is already set for the subgroup on EUCI sharing and exchange of classified information and could be expanded to other subgroups.

D. Organisation of security – Article 8

15. It should be left up to each institution and body organise the necessary administrative support to their Security Authority.

16. The Security Authority of each EUIBA should not assume the functions as described in article 8(3) and (4), but be entitled to establish them.

17. It could be considered to move the functions of the Security Authorities as described in article 8(3)(c),(d) and (f) to the CIS part of the Regulation (Chapters 3 or 5).

18. It should be made clear that each EUIBA should avoid conflicts of interests between individuals or entities entrusted with these security functions.

19. The function of the Crypto Approval Authority as described in article 8(3)(e) should be deleted since the list of approved cryptos should be centrally established.

20. The provisions in article 8(4) are deemed sufficient to allow for a voluntary centralisation of security functions.

III. Conclusion

21. The Council Security Committee is invited to consider the proposals as set out above and have a first exchange of views of the suggested redraft for Articles 6-8 as set out in the Annex II to this note.

ANNEX II

Article 6

Interinstitutional Information Security Coordination Group

1. An Interinstitutional Information Security Coordination Group (the 'Coordination Group') is established. ~~It shall be composed of the representatives of all Security Authorities of the Union institutions and bodies, and shall have a mandate to define their common policy in the field of information security.~~

1a. The Coordination Group shall be responsible for monitoring the implementation of this Regulation by the Union institutions and bodies and establishing guidance in the field of information security.

1ab. The Coordination Group shall consist of:

a) one representative designated by each of the following:

(i) the European Parliament;

(ii) the European Council;

(iii) the Council of the European Union;

(iv) the European Commission;

(v) the Court of Justice of the European Union;

(vi) the European Central Bank;

(vii) the European Court of Auditors;

(viii) the European External Action Service;

(ix) the European Economic and Social Committee;

(x) the European Committee of the Regions;

(xi) the European Investment Bank;

(xii) the European Defence Agency (EDA);

(xiii) the European Union Agency for Criminal Justice Cooperation (Eurojust);

(xiv) the European Union Agency for Law enforcement Cooperation (Europol);

(xv) European Union Agency for the Space Programme (EUSPA);

(xvi) the European Border and Coast Guard Agency (Frontex);

(xvii) the European Union satellite centre (SatCen);

b) three representatives designated by the Union Agencies Network (EUAN) to represent the interests of the agencies and bodies.

1ac. Members may be assisted by an alternate. Other representatives of the institutions and bodies listed above or of other Union entities may be invited by the chair to attend specific meetings or part thereof of the Coordination Group.

2. **The Coordination Group shall ac**~~ting~~ by ~~consent~~ **consensus** and in the common interest of all Union institutions and bodies~~, the Coordination Group shall.~~**.**

2a. The Coordination Group shall:

(a) adopt its rules of procedure**;** ~~and~~

(aa) adopt its annual common objectives and priorities;

(b) adopt decisions on the establishment of thematic sub-groups and their terms of reference;

(c) establish guidance documents on the implementation of this Regulation, in cooperation, **where appropriate**, with the Interinstitutional Cybersecurity Board referred to in Article 9 of the Regulation EU [...] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, ~~where appropriate;~~

(ca)receive reports from the thematic subgroups including, as appropriate, any recommendations for establishing guidance documents;

(d) set up dedicated platforms for sharing best practices and knowledge on common topics relevant to information security as well as for providing assistance in case of information security incidents;.

~~(e) ensure that security measures are coordinated as necessary with the competent National Security Authorities for the purpose of protecting EUCI.~~

3. The Coordination Group shall designate a chairperson and two vice chairpersons from among ~~its members~~ **the representatives of the European Parliament, the Council and the Commission,** for a period of **2**~~3~~ years, **in accordance with its rules of procedure**.

4. The Coordination Group shall in principle meet at least ~~once a year~~ **three times a year** at the initiative of its chairperson or at the request of a Union institution or body.

4a. The Coordination Group may act by a simplified written procedure initiated in accordance with its internal rules of procedure. Under that procedure, the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects.

5. The Coordination Group shall have the administrative support of a permanent secretariat provided by the Commission.

~~6. Each Union institution or body shall be appropriately represented in the Coordination Group and where applicable, in the thematic sub-groups~~.

7. Union institutions and bodies shall ~~bring to the attention of~~ **inform** the Coordination Group **of** any significant information security policy development within their organisation.

Article 6a (new)

Information Security Committee

~~8~~**1**. ~~In the performance of the tasks referred to in paragraph (2), point (e), the Coordination Group shall be assisted by an Information Security Committee.~~ **An Information Security Committee is established to ensure that the guidance defined by the Coordination Group is coordinated with the [competent authorities of the Member States] [with the National Security Authorities for protecting classified information].**

2. The~~at~~ **Information Security** Committee shall be composed of one representative from each National Security Authority and shall **be chaired by a representative of the Council.**

3. **The European Parliament, the Commission and the European External Action Service shall be invited to take part in the meetings of the Information Security Committee**. **Other Union institutions and bodies may be invited on a case by case basis at the initiative of its chairperson or at the request of one of its members.**

4. **The Information Security Committee shall have the administrative support provided by the Council.** ~~be chaired by the Secretariat of the Coordination Group, referred to in paragraph (5).~~

5. ~~The Information Security Committee shall have an advisory role.~~ **The Information Security Committee shall be consulted by the Coordination Group [and thematic subgroups] and shall provide advice on any envisaged guidance the implementation of which could have an impact for Member States or require their contribution.**

6. **The Information Security Committee shall meet at the initiative of its chairperson or at the request of one of its members.**

Article 7

Thematic sub-groups

1. The Coordination Group shall set up the following permanent thematic sub-groups to facilitate the implementation of this Regulation:

(a) a sub-group on information assurance;

[(b) a sub-group on non-classified information;**]**

(c) a sub-group on physical security;

(d) a sub-group on accreditation of communication and information systems handling and storing EUCI;

(e) a sub-group on EUCI sharing and exchange of classified information.

2. Where necessary, the Coordination Group may set up ad-hoc sub-groups for a specific task and for a limited duration.

3. Except where otherwise provided in **this Regulation or** their terms of reference, the sub-groups shall be based on open membership representing the Union institution or body concerned. The members of the sub-groups shall be experts in the respective field of competence.

4. The ~~S~~**s**ecretariat of the Coordination Group, referred to in Article **6**~~5~~(5), shall support the work of all sub-groups and ensure the communication between its members.

Article 8

Organisation of security

1. Each Union institution and body shall designate a Security Authority to assume the responsibilities assigned by this Regulation and, where applicable, by its internal security rules. ~~In performing its tasks, each Security Authority shall have the support of the department or officer entrusted with Information Security tasks.~~

2. Where necessary, ~~the Security Authority of~~ each Union institution and body shall adopt internal implementing rules for the protection of information, in accordance with their specific mission, as entrusted by the EU law, and ~~based on~~ **in full respect of** their institutional autonomy.

3. Where relevant, ~~each Security Authority shall also assume the following functions~~ **the following functions shall also be established by the Security Authority of each Union institution and body**:

(a) Information Assurance Authority in charge of developing information assurance security policies and security guidelines and monitoring their effectiveness and pertinence;

(b) Information Assurance Operational Authority responsible for developing security documentation, in particular the Security Operating Procedures and the crypto plan within the communication and information systems accreditation process;

(c) Security Accreditation Authority in charge of accrediting Secured Areas and CIS handling and storing EUCI;

(d) TEMPEST Authority responsible for approving the measures taken to protect against compromise of EUCI through unintentional electronic emanations;

~~(e) Crypto Approval Authority responsible for approving the use of encrypting technologies, based on a request from the system owner;~~

(~~f~~**e**) Crypto Distribution Authority responsible for distributing cryptographic materials used for protecting EUCI (encryption equipment, cryptographic keys, certificates, and related authenticators) to the users concerned.

4. The **Security Authority of each institution and body may delegate** ~~responsibilities of~~ one or more of the functions referred to in paragraph 3 ~~may be delegated~~ to another Union institution or body whenever decentralised delivery of security offers significant efficiency, resource or time savings.

4a. Conflicts of interest between the persons or entities entrusted with the functions referred to in paragraph 3 shall be avoided.