Council of the European Union

Brussels, 26 June 2023
(OR. en)

8453/1/23
REV 1

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 revised version of Articles 6, 7 and 8 of the draft Regulation following the discussions at the CSC meeting on 5 May 2023. Changes compared to the previous version are indicated in **bold underlined** and deletions in ~~strikethrough~~.

The main outstanding issues include the composition of the Interinstitutional Information Security Coordination Group (IISCG) and the relationship between the IISCG and the Information Security Committee. Delegations have also expressed the need to further strengthen the role of the Member States in the envisaged governance structure.

These issues will be discussed at the CSC meeting on 5 July 2023.

ANNEX

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

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 with regard to the implementation of this Regulation.**

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 Data Protection Supervisor;

(xiii) the European Ombudsman;

(xiv) the European Public Prosecutor Office;

~~**(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.~~**.**

2~~a~~b. 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;

(ba) consult the Information Security Committee on any matter which could have an impact on the Member States or require their contribution and take utmost account of the advice provided by the Information Security Committee;

(c) establish guidance documents on the implementation of this Regulation, in cooperation **with the Information Security Committee and, 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; the Coordination Group may also request reports or recommendations from the thematic subgroups if deemed necessary.

(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 and based on the principle of rotation between these institutions**.

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~~]~~ or with other relevant national competent authorities.**

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 Information Security Committee shall adopt its internal rules of procedure.

~~3~~**4.** **[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~~**5.** **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~~**6.** ~~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~~ may provide advice on any envisaged guidance the implementation of which could have an impact for Member States or require their contribution. The Committee may decide not to give an opinion if it considers that the matter in question does not require it.**

~~6~~7. 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.