COUNCIL OF THE EUROPEAN UNION

Brussels, 30 May 2011

10872/11

LIMITE

CSC 30

"I/A" ITEM NOTE

From:	The Security Committee
To:	COREPER/Council
No. prev. doc.:	15104/10
Subject:	Policy on creating EU classified information

1. In line with Article 3(3) and Article 6(1) of the Council security rules[1], the Security Committee has developed a draft policy on creating EU classified information (EUCI), including a practical classification guide, and agreed on it on 23 May 2011.

2. The policy lists the entities which may create EUCI and provides guidance on how to classify information as EUCI.

3. Subject to confirmation by COREPER, the Council is accordingly invited to approve the attached policy.

---

[1] Council Decision 2011/292/EU of 31 March 2011, OJ L 141, 27.5.2011, p. 17.

ANNEX

POLICY ON CREATING EU CLASSIFIED INFORMATION

I. Introduction

1. This policy, approved by the Council in accordance with Article 3(3) of the Council Security Rules[1] (hereafter the 'CSR'), lays down general standards for protecting EUCI. It constitutes a commitment to help achieve an equivalent level of implementation of the CSR.

2. This policy lists the entities which may create EUCI and provides guidance on how to classify information as EUCI.

3. The Council and the General Secretariat of the Council (GSC) will apply this security policy with regard to protecting EUCI in their premises and communication and information systems (CIS).

4. The Member States will act in accordance with national laws and regulations to the effect that the standards laid down in this security policy with regard to protecting EUCI are respected when EUCI is handled in national structures, including in national CIS.

II. Definition of EUCI and EU security classifications

5. According to Article 2(1) of the CSR, EUCI means "any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States". The EU security classifications referred to in this definition and the corresponding descriptions are the following[2]:

---

1 Council Decision 2011/292/EU of 31 March 2011, OJ L 141, 27.5.2011, p. 17

2 Article 2(2) of the CSR

(a) TRES SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

(b) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

(d) RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

III. Originators of EUCI

6. In accordance with the CSRs, "originator" means the EU institution, agency or body, Member State, third State or international organisation under whose authority classified information has been created and/or introduced into the EU's structures.

7. The EU institutions, agencies, bodies and entities referred to hereafter may create EUCI, as follows:

(a) all classified information created by the European Council, the Council or the GSC is designated and marked as EUCI in accordance with the CSR;

(b) all classified information created by the European Commission or by the Commission services is designated and marked as EUCI in accordance with the relevant security provisions[1];

(c) all classified information created by the European External Action Service (EEAS) is designated and marked as EUCI in accordance with the security rules for the EEAS;

[1] Commission Decision 2001/844/EC, ECSC, Euratom, OJ L 317, 3.12.2001, p. 1

(d) where the founding acts of EU agencies and bodies provide for them to apply the CSR or the Commission's security provisions, all classified information created by them is designated and marked as EUCI;

(e) all classified information created by the European Police Office (Europol) is designated and marked as EUCI in accordance with the rules on the confidentiality of Europol information;[1]

(f) all classified information created by:

- EU missions established by the Council under the Common Security and Defence Policy (CSDP), or by
- EU Special Representatives (EUSRs) and their teams,

is designated and marked as EUCI in accordance with the Council Decisions establishing their mandates.

8. Member States may create EUCI in the context of the EU's activities. This is without prejudice to the possibility for them to introduce classified information bearing a national security classification marking into the structures or networks of the EU. In the latter case, the Council and the GSC, as well as EU agencies and bodies which apply the CSR, will protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix B to the CSR.

9. Where delegations feed classified information into the EU's decision-making process in the European Council or Council in the form of amendments to or comments on official European Council or Council documents originating in the GSC, they will mark such information as EUCI and not as national classified information. In this specific case, the function of originator with regard to such EUCI will be exercised by the Council.

[1] Council Decision 2009/968/JHA of 30 November 2009, OJ L 332, 17.12.2009, p. 17.

10. The originator retains control of EUCI which it has created. This means that its prior written consent must be sought before EUCI is:

(a) downgraded or declassified;

(b) used for purposes other than those established by the originator;

(c) disclosed to any third State or international organisation;

(d) disclosed to a contractor or prospective contractor located in a third State;

(e) copied or translated, in case the information is classified TRES SECRET UE/EU TOP SECRET.

IV. Classifying

11. Only authorised entities and functions within the GSC and Member States may create and classify information as EUCI, in particular at the level CONFIDENTIEL UE/EU CONFIDENTIAL and above.

12. Classifying information as EUCI involves an assessment and a decision by the originator that the disclosure of such information to unauthorised persons would cause a degree of prejudice to the interests of the European Union or of one or more of the Member States as described in paragraph 5 above. Such decisions must not be taken lightly; due consideration must be given to the actual content and sensitivity of the information before deciding that it needs to be classified.

13. Once a decision has been made to classify the information, an assessment must be made of the classification level warranted by it. The practical classification guide attached in Annex I contains criteria on the basis of which classification decisions should be taken.

14. The classification level assigned to the information determines the level of protection afforded to it in the areas of personnel security, physical security, procedural security and information assurance. Annex II summarises the security measures applied to each security classification level in accordance with the CSR. Security measures increase substantially the higher the classification is.

15. Information which warrants classification must be marked and handled as such regardless of its physical form. Its classification must be clearly communicated to its recipients, either by a classification marking (if it is delivered in written form, be it on paper or in CIS) or by an announcement (if it is delivered in oral form, such as in a conversation or a presentation). Classified material should be physically marked so as to allow for its security classification to be easily identified.[1]

16. EUCI in electronic form may only be created on CIS accredited by the competent Security Accreditation Authority. The classified information itself as well as the filename and storage device (if external, such as CD-ROMs or USB sticks) must bear the relevant security classification marking.

17. Information should be classified as soon as it takes form. For example, personal notes, drafts or e-mail messages containing information which warrants classification are to be marked as EUCI from the outset and should be produced and handled in accordance with the requirements of the CSR in physical and technical terms. Such information may then evolve into an official document which will in turn be appropriately marked and handled. During the drafting process an official document may need to be re-evaluated and assigned a higher or lower classification level as it evolves.

18. Originators may decide to attribute a standard classification level to categories of information which they create on a regular basis. However, they must ensure that in so doing they do not systematically overclassify or underclassify individual pieces of information (see Section VI below, "Overclassication and underclassification").

[1] Details on marking EUCI are contained in the "Guidelines on Marking EUCI" approved by the Council Security Committee (doc. 10873/11).

V. Classifying compilations, cover pages, excerpts

19. The overall classification level of a document or file will be at least as high as that of its most highly classified component. For example, a document or file containing unclassified components and SECRET UE/EU SECRET components will be classified SECRET UE/EU SECRET.

20. When information from various sources is collated, the final product will be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

21. The classification of a letter or note covering enclosures will be as high as the highest classification of its enclosures. The originator will indicate clearly at which level it is classified when detached from its enclosures.[1]

22. Documents or files containing components with different classification levels are to be structured whenever possible so that components with a different classification level may be easily identified and detached if necessary.

23. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and are to be marked accordingly, including when stored in electronic form. Standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page.[2]

---

1 See CSR, Annex III, paragraph 9, and "Guidelines on marking EUCI".
2 See CSR, Annex III, paragraph 12, and "Guidelines on marking EUCI".

VI. Overclassification and underclassification

24. Information should be classified at the level which corresponds to the degree of prejudice its unauthorised disclosure could cause: not higher, not lower.

25. Overclassification means attributing a classification level higher than that warranted for a given piece of information. Overclassification is to be avoided, since it puts an unnecessary (or even counterproductive) burden on the handling of the information and entails unnecessary costs.

26. Underclassification means attributing a classification level lower than that warranted for a given piece of information. Underclassification is to be avoided, since it exposes the information to increased risk of disclosure to unauthorised persons.

VII. Downgrading and declassification

27. Classification is to be maintained only as long as the information requires protection. When creating a document, the originator should indicate where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether the document can be downgraded or declassified on a given date or following a specific event.

VIII. Initial distribution and further distribution

28. The originator establishes the initial "need-to-know" for the EUCI it has created by drawing up a distribution list.

29. Information classified RESTREINT UE/EU RESTRICTED can be distributed by the originator. For information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, the distribution list (and any further instructions on distribution) is to be provided to the relevant registry, which will register and distribute the information.

30. Information classified up to SECRET UE/EU SECRET may be further distributed on instruction from the holder, provided that the originator has not imposed caveats on such further distribution. Information classified TRES SECRET UE/EU TOP SECRET may only be further distributed with the prior written consent of the originator.

Practical classification guide

If the unauthorised disclosure of the document you are creating could…	i.e.	then you should classify it as…
be disadvantageous to the interests of the European Union or of one or more of the Member States	• adversely affect diplomatic relations • cause substantial distress to individuals • make it more difficult to maintain the operational effectiveness or security of Member States' or other contributors' deployed personnel • cause financial loss or facilitate improper gain or advantage for individuals or companies • breach undertakings to maintain the confidence of information provided by third parties • breach statutory restrictions on disclosure of information • prejudice the investigation or facilitate the commission of crime • disadvantage EU or Member States in commercial or policy negotiations with others • impede the effective development or operation of EU policies • undermine the proper management of the EU and its missions	RESTREINT UE/EU RESTRICTED
harm the essential interests of the European Union or of one or more of the Member States	• materially damage diplomatic relations, i.e. cause formal protest or other sanctions • prejudice individual security or liberty • cause damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the effectiveness of valuable security or intelligence operations • substantially undermine the financial viability of major organisations • impede the investigation or facilitate the commission of serious crime • work substantially against EU or Member States financial, monetary, economic and commercial interests • seriously impede the development or operation of major EU policies • shut down or otherwise substantially disrupt significant EU activities	CONFIDENTIEL UE/EU CONFIDENTIAL

If the unauthorised disclosure of the document you are creating could…	i.e.	then you should classify it as…
seriously harm the essential interests of the European Union or of one or more of the Member States	• raise international tensions • seriously damage relations with third States or international organisations • threaten life directly or seriously prejudice public order or individual security or liberty • cause serious damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of highly valuable security or intelligence operations • cause substantial material damage to EU or one of its Member States financial, monetary, economic and commercial interests	SECRET UE/EU SECRET
cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States	• threaten directly the internal stability of the EU or of one or more of its Member States or third States or international organisations • cause exceptionally grave damage to relations with third States or international organisations • lead directly to widespread loss of life • cause exceptionally grave damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of extremely valuable security or intelligence operations • cause severe long-term damage to the EU or Member States' economy.	TRES SECRET UE/EU TOP SECRET

ANNEX II

Summary of security measures

This table summarises the security measures which apply to documents classified in accordance with the Council security rules. The contents of this table are purely indicative and do not replace the content of the security rules themselves, nor of security policies or guidelines implementing them.

	RESTREINT UE/ EU RESTRICTED	**CONFIDENTIEL UE /EU CONFIDENTIAL**	**SECRET UE/ EU SECRET**	**TRES SECRET UE/ EU TOP SECRET**
Need-to-know	Yes	Yes	Yes	Yes
Security clearance	No	Yes	Yes	Yes
Registration for security purposes	No	Yes	Yes	Yes
Initial distribution	Determined by originator through a distribution list; distribution may be carried out by originator	Determined by originator through a distribution list; distribution carried out by the relevant registry	Determined by originator through a distribution list; distribution carried out by the relevant registry	Determined by originator through a distribution list; distribution carried out by the relevant TRES SECRET UE/EU TOP SECRET registry
Copying, translation, further distribution	On instruction from the holder, unless otherwise specified by the originator	By the relevant registry, on instruction from the holder, unless otherwise specified by the originator	By the relevant registry, on instruction from the holder, unless otherwise specified by the originator	By the relevant TRES SECRET UE/EU TOP SECRET registry, subject to originator's prior written consent
Physical protection for handling	In administrative or secured areas, or outside such areas under conditions to be laid down by the competent security authority	In administrative or secured areas, or outside such areas under conditions to be laid down by the competent security authority	In administrative or secured areas, or outside such areas under conditions to be laid down by the competent security authority	Only in secured areas

	RESTREINT UE/ EU RESTRICTED	**CONFIDENTIEL UE /EU CONFIDENTIAL**	**SECRET UE/ EU SECRET**	**TRES SECRET UE/ EU TOP SECRET**
Physical protection for storage	In administrative or secured areas, or temporarily outside such areas under conditions to be laid down by the competent security authority	Only in secured areas	Only in secured areas	Only in secured areas
Physical measures for storage	In suitable locked office furniture	In an approved security container or strong room	In an approved security container or strong room	In an approved security container or strong room, subject to additional security measures
CIS for handling and storing	Accredited	Accredited	Accredited	Accredited
TEMPEST measures	No	Yes	Yes	Yes
Carriage within a building or self-contained group of buildings	Covered from view	Covered from view	Covered from view	In a secured envelope
Carriage within the EU	- Military, government or diplomatic courier - Hand carriage (under conditions); - Postal/ commercial courier services (under conditions)	- Military, government or diplomatic courier; - Hand carriage (under conditions); - Postal or commercial courier services (under conditions)	- Military, government or diplomatic courier; - Hand carriage (under conditions); - Postal or commercial courier services (under conditions, and only within a Member State)	Military, government or diplomatic courier only

	RESTREINT UE/ EU RESTRICTED	**CONFIDENTIEL UE /EU CONFIDENTIAL**	**SECRET UE/ EU SECRET**	**TRES SECRET UE/ EU TOP SECRET**
Carriage from within the EU to the territory of a third State	- Military, government or diplomatic courier; - Hand carriage (under conditions); - Postal or commercial courier services (under conditions)	- Military, government or diplomatic courier; - Hand carriage (under conditions)	- Military, government or diplomatic courier; - Hand carriage (under conditions)	Military or diplomatic courier only
Transmission by electronic means	Encrypted with approved devices	Encrypted with approved devices	Encrypted with approved devices	Encrypted with approved devices
Destruction	By holder, using approved methods	By registry, using approved methods	By registry, using approved methods and in the presence of a witness	By registry, using approved methods and in the presence of a witness