COUNCIL OF THE EUROPEAN UNION

Brussels, 11 November 2011

16751/11

CSC 75

"I/A" ITEM NOTE

From:	The Security Committee
To:	COREPER/Council
Subject:	Policy on registration for security purposes

1. In line with Annex III, paragraph 22 of the Council security rules[1], the Security Committee has developed a draft policy on registration for security purposes and agreed on it on 4 November 2011.

2. The policy provides details on the establishment and structure of the registries handling EUCI as well as on different types of procedures to be carried out by such registries.

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 REGISTRATION FOR SECURITY PURPOSES

I. INTRODUCTION

1. This policy, approved by the Council in accordance with Annex III, paragraph 22, of the Council Security Rules[2] (hereinafter 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. The general standards laid down in this policy provide details on the following:

   (a) the establishment and structure of the registries handling EUCI;

   (b) the registration, traceability, handling, distribution, copying, translation, review, downgrading, declassification, destruction and archiving of EUCI;

   (c) the frequency of audits and inventories; and

   (d) procedures for reporting a breach or suspected breach of security.

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.

---

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

5. EU agencies and bodies established under Title V, Chapter 2, of the TEU, Europol and Eurojust should use this security policy as a reference for implementing security rules in their own structures.

II. DEFINITIONS

6. (a) "EU classified information" ("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 (CSR, Article 2(1)).

(b) "Document" means any recorded information regardless of its physical form or characteristics (CSR, Appendix A).

(c) "Organisational entity" means a unit/department within which EUCI is handled.

(d) "CIS" means any system enabling the handling of EUCI in electronic form (CSR, Article 10(2)).

(e) "Registration for security purposes", hereinafter "registration", means the application of procedures which record the life-cycle of EUCI, including its dissemination and destruction (CSR, Annex III, paragraph 18).

(f) "Secured Area" means an area which, after being inspected by the competent security authority, has been certified by that authority as complying with the requirements of the CSR (CSR, Article 8(4)).

(g) "Logbook" means a register which records when EUCI enters or exits a registry, is accessed by or transmitted to a security-cleared person and/or is destroyed. A logbook can be either paper-based or implemented in a CIS.

III. REGISTRY STRUCTURE

7. In accordance with the CSR[3], for every organisational entity within the GSC and Member States' national administrations in which EUCI is handled, a registry will be identified to ensure that EUCI is handled in accordance with the CSR. Registries will be established as Secured Areas as defined in Annex II of the CSR.

8. In accordance with the CSR[4], the GSC and each Member State will designate a registry to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET.

9. For the GSC, this will be the Central Registry, whose head will be the GSC's Chief Registry Officer.

10. Each National Security Authority (NSA) will notify the GSC of the registry designated for the purposes of paragraph 8 above. This registry will be the single point of contact for the GSC in the Member States on matters relating to the registration of EUCI and to the registry structure within that Member State, unless otherwise specified by the NSA.

11. The GSC and each Member State may create a structure of sub-registries, as required, in order to ensure the correct management of EUCI and facilitate the handling of EUCI within their structures.

12. In accordance with Annex I of the CSR, staff working in registries and sub-registries will be appropriately security-cleared to handle the maximum classification level of EUCI entrusted to them.

---

3 Annex III, paragraph 17.
4 Annex III, paragraph 23.

IV. REGISTRATION PROCEDURE

13. The originator of EUCI will be responsible for determining the appropriate security classification level in accordance with the policy on creating EUCI[5] and for the initial registration of the EUCI in question.

14. All information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above will be registered for security purposes in designated registries.

15. Such information will be registered:
    – when it arrives at or leaves an organisational entity; and
    – when it arrives at or leaves a CIS,
    in order to ensure constant traceability.

16. The central registry of the GSC will keep a record of all EUCI released by the Council and the GSC to third States and international organisations, and of all classified information received by the Council and the GSC from third States and international organisations.

17. Registration may be carried out in paper or in electronic logbooks. Logbooks should record at least the following information:

    (a) when EUCI enters the registry;

    (b) the document title, classification level, and any reference number assigned to the document;

    (c) details of the originator;

    (d) a record of who is given access to the document, and when it was accessed;

    (e) a record of any copies or translations made;

[5] Doc. 10872/11.

(f) when EUCI, or any copies or translations thereof, leave the registry, and details of where it has been sent; and

(g) when EUCI was destroyed, and by whom, in accordance with the CSR[6].

18. Logbooks may be classified as appropriate. Logbooks where information classified TRES SECRET UE/EU TOP SECRET is registered will as a general rule be classified.

19. Classified information may be registered:

(a) in a single logbook; or

(b) in separate logbooks according to its classification level, to whether it is incoming or outgoing and to its origin or destination.

20. In the case of electronic handling within a CIS, registration procedures may be performed by processes within the CIS itself which meet requirements equivalent to those specified above. Whenever EUCI leaves the perimeter of the CIS, the registration procedure described above applies.

V. INITIAL DISTRIBUTION

21. Registries will distribute EUCI in accordance with the CSR following the instructions of the originator, taking into account the security-clearance status of the recipients.

[6] Annex III, paragraphs 41-46.

VI. COPYING / TRANSLATING REGISTERED EUCI

22. In accordance with the CSR[7], documents classified TRES SECRET UE/EU TOP SECRET may only be copied or translated with the prior written consent of the originator. Documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be copied or translated on instruction from the holder, provided the originator has not imposed caveats not permitting this.

23. Each copy of a document classified TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET EU or CONFIDENTIEL UE/EU CONFIDENTIAL must be registered. The security measures applicable to the original document will apply equally to copies and translations thereof.

24. Requests for copies and/or translations of EUCI can be made by the originator or copy holder to the relevant registry or sub-registry, in accordance with the CSR. Copies may only be produced in a secured area and on copiers which are part of an accredited CIS. All copies and translations must be appropriately marked, numbered and registered.

VII. REVIEWING THE CLASSIFICATION LEVEL OF REGISTERED EUCI

25. Originators of EUCI will indicate, where possible, whether EUCI can be downgraded or declassified on a given date or following a specific event. When it is not practicable to provide such information, the GSC central registry will review the classification level of EUCI held by it no less frequently than every five years. The downgrading and declassification of such EUCI is subject to the prior written consent of the originator. If the originator cannot be established or traced, the Council will assume the former's responsibility.

---

7 Annex III, paragraphs 25-27.

VIII. DOWNGRADING REGISTERED EUCI

26. The registry responsible for downgrading must inform recipients of the initial document of its new classification level.

27. After downgrading, the document will be registered in the logbooks corresponding to both the old and the new classification level. The date of downgrading must be recorded, as well as the name of the person who authorised it.

28. The downgraded document and all copies of it must be marked with the new classification level and stored appropriately.

IX. DECLASSIFYING EUCI

29. A registry which carries out a total or partial declassification of EUCI must inform recipients of the original document that it has been declassified.

Total declassification

30. When EUCI is declassified, it must be recorded in the logbook with the following data: date of declassification, name of the person who requested and authorised it, reference number of the declassified document and its final destination.

31. The old classification markings in the declassified document and in all its copies must be struck through. The document and all copies of it must be stored appropriately.

Partial declassification

32. Upon partial declassification of a classified document, a declassified extract will be produced and stored appropriately. The relevant registry must register: the date of the partial declassification, the name of the person who requested and authorised it and the reference number of the declassified extract.

X. DESTROYING REGISTERED EUCI

33. Destruction of registered EUCI must be recorded in the relevant logbook with the following data: date/time, name of the person who authorised it, name of the person who carried out the destruction, identification of the document or copies destroyed, physical form in which the destroyed EUCI had been stored, means of destruction, place of destruction.

34. A destruction certificate must be produced in accordance with the CSR[8] and archived in place of the destroyed EUCI. The registry must keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for at least ten years and of SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL documents for at least five years.

XI. PERIODIC AUDIT AND INVENTORY

35. The person responsible for a registry must produce, at least annually, an inventory of classified information kept in the registry and report on it to the registry to which it is accountable. When the person responsible is replaced, the new person responsible must produce a full inventory of the registry, reporting to the registry to which it is accountable.

36. The person responsible for a registry which has subordinate registries must carry out an administrative audit of the inventories of the subordinate registries at least annually.

XII. REPORTING SECURITY BREACHES

37. Any breach or suspected breach of security is to be reported immediately to the competent security authority in accordance with approved procedures.

---

[8] Annex III, Section VI.