COUNCIL OF THE EUROPEAN UNION

Brussels, 28 August 2007

12142/07

LIMITE

CSC 27
PESC 944
JAI 411

NOTE

From :	The General Secretariat of the Council
To :	Delegations
Subject :	Security Arrangement for the protection of classified information exchanged between the EU and the United States of America under the EU-US Agreement on the security of classified information

Delegations will find attached the Security Arrangement for the protection of classified information exchanged between the EU and the United States of America under the Agreement between the European Union and the government of the United States of America on the security of classified information (OJ L 115, 03.05.2007, p. 30).

The Arrangement was approved by the Council Security Committee on 29 June 2007 and by the US on 18 July 2007.

It should be noted that:

- the transmission of EU classified documents to the US is allowed up to the level TRES SECRET UE/EU TOP SECRET; and
- the transmission of EU classified information to the US by electromagnetic means is limited to the level CONFIDENTIEL UE until a future follow-up evaluation visit recommends that classified information of a higher level may be exchanged.

SECURITY ARRANGEMENT BETWEEN THE EU COUNCIL GENERAL SECRETARIAT SECURITY OFFICE (GSCSO) AND THE EUROPEAN COMMISSION SECURITY DIRECTORATE (ECSD) AND THE UNITED STATES DEPARTMENT OF STATE FOR THE PROTECTION OF CLASSIFIED INFORMATION EXCHANGED BETWEEN THE EU AND THE UNITED STATES OF AMERICA

INTRODUCTION

1. Pursuant to Article 13 of the Agreement between the Government of the United States of America (USG) and the European Union (EU) on security procedures for the exchange of classified information (the Agreement), reciprocal standards for the protection of classified information exchanged between USG and the EU are hereby mutually accepted. The United States Department of State, the GSCSO and the ECSD ("the participants") are responsible for the implementation and oversight of these standards.

2. Each participant is to notify the other in writing that the necessary security measures have been put in place in accordance with this arrangement before any classified information is exchanged.

3. The participants will make their best effort to implement fully the elements contained in this Arrangement.

PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS

4. Each facility or establishment that contains classified information released or exchanged by the other participant is to maintain an inventory of individuals at the facility or establishment who are authorised to have access to classified information.

5. Before being given access to classified information, all individuals who require access to classified information are to be briefed on the protective security regulations relevant to the classification of the information they are to access. Those individuals accessing classified information are to be made aware that any breach of the security regulations may result in disciplinary action and/or possible further legal action in accordance with the Parties' respective laws and regulations.

CLASSIFICATION SYSTEM

6. Classification markings as set out in Article 3 of the Agreement, are to be used to indicate the sensitivity of the classified information and thus the security procedures and regulations which apply for its protection.

7. Within the USG, information classified RESTREINT UE is to be handled on a "need to know basis" and is to be afforded a level of protection at least equivalent to that foreseen in the Council's security regulations. The USG may apply appropriate procedures and caveats to ensure that such special handling instructions are observed.

8. All information originated by one of the participants and provided to the other(s) - is to include an express releasability marking, such as:

SECRET
RELEASABLE TO THE EU

SECRET UE
RELEASABLE TO THE USA

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

Registries

9. A registry system is to be established in the U.S. Department of State, the General Secretariat of the Council and the European Commission for the receipt, dispatch, control and storage of classified information subject to the Agreement.

10. Registries are to be responsible for:

(a) distribution and control of classified information in accordance with the following provisions:

(i) Information classified CONFIDENTIEL UE or CONFIDENTIAL and above arriving at or leaving the designated registry acting as the point of entry and exit for classified information is to be recorded in a logbook or in a special protected computer media, indicating the date received, particulars of the document (date, reference and copy number), the subject of the document, the classification level, the title, the addressee's name or title, the date of return of the receipt and the date of return of the document to EU or the USG, its distribution to other registries or its destruction.

(ii) Information classified CONFIDENTIEL UE or CONFIDENTIAL and above may only be handled, distributed and consulted in a special security area in such a way that it can be protected from access by unauthorised persons by means of internally established controls: e.g. premises containing offices in which CONFIDENTIEL UE or CONFIDENTIAL and above is regularly handled and stored.

(iii) Around the security area an administrative area of lesser security may be established. Only RESTREINT UE information is to be handled and stored in administrative areas.

(b) the storage of information classified CONFIDENTIEL UE or CONFIDENTIAL or above in a special area of the registry. The classified information is to be stored in security containers or locked security cabinets, the specifications of which are in accordance with the respective laws and regulations of the Parties to the Agreement.

(c) the final disposition (including return if so requested) and/or downgrading and/or declassification of classified information, subject to the written consent of the originator, including the maintenance of destruction certificates for classified information from the USG or the EU.

11. The U.S. Department of State, GSCSO and ECSD are to be responsible for the oversight and control of registries within their respective administrations and are to inform their counterparts of the establishment/disestablishment of registries containing each other's classified information.

Storage

12. Information classified CONFIDENTIEL UE or CONFIDENTIAL and above is to be stored in security containers corresponding to the respective laws and regulations of the participants, in special security areas.

13. Information classified RESTREINT UE is to be handled in premises that are not accessible to unauthorised personnel and stored in locked containers.

14. All classified information, regardless of media, is to be stored in a secure manner.

Copying

15. Information classified SECRET UE or SECRET and above may be reproduced or copied only with the releasing participant's prior written consent.

16. When classified documents or media containing classified information are reproduced, all original security markings thereon are also to be reproduced or marked on each copy. Such reproduced documents or media are to be placed under the same protection as the original document or media. The number of copies is to be limited to that required for official purposes

17. Copy machines are to be protected to avoid unauthorised reproducing of extra copies. The security classification on classified information reproduced or copied are to correspond to the security classification of the original information.

Destruction

18. Classified documents or media containing classified information received from the releasing Participant are to be destroyed in an appropriate manner or returned to the releasing participant for destruction, to prevent reconstruction of the classified information contained therein.

19. Classified material, including equipment, containing classified information in whole or in part, is to be destroyed so that it is no longer recognisable and so as to preclude reconstruction of the transmitted classified information in whole or in part.

20. In the case of CONFIDENTIEL UE or CONFIDENTIAL documents, an appropriate note is to be entered in the special registers. In the case of SECRET UE or SECRET and above documents, destruction certificates are to be issued and signed by two appropriately security cleared persons witnessing their destruction. These certificates are to be retained for at least three years.

MANUAL TRANSMISSION OF CLASSIFIED INFORMATION BETWEEN THE PARTICIPANTS

21. When exchanging information classified CONFIDENTIEL UE or CONFIDENTIAL and above, appropriately cleared couriers are to be used by both sides. Upon presentation of the appropriate security clearance certificate, such couriers are to be granted access badges to the building(s) they need to visit to deliver and collect the documents.

22. Documents

(a) Documents or media containing classified information are to be transmitted in double, sealed envelopes, the innermost envelope bearing only the classification of the documents or other media and the organisational address of the intended recipient, and the outer envelope bearing the organisational address of the recipient, the organisational address of the sender, and the registry number, if applicable.

(b) No indication of the classification of the enclosed documents or media is to be made on the outer envelope. The sealed envelope is then to be transmitted according to the prescribed procedures of the participants.

(c) Receipts are to be prepared for packages containing classified documents or media that are transmitted between the participants, and a receipt for the enclosed documents or media is to be signed by the final recipient and returned to the sender.

23. Classified material

(a) Classified material, including equipment, is to be transported in sealed, covered vehicles, or be securely packaged or protected in order to prevent identification of its details, and kept under continuous control to prevent access by unauthorised persons.

(b) Classified material, including equipment, which must be stored temporarily awaiting shipment is to be placed in protected storage areas. The areas are to be protected by intrusion-detection equipment or guards with security clearances who are to maintain continuous surveillance of the storage areas. Only authorised personnel with the requisite security clearance may have access to the storage areas.

(c) Receipts are to be obtained on every occasion when classified material, including equipment, changes hands en route, and a receipt is to be signed by the final recipient and returned to the sender.

LOSSES OR COMPROMISES OF SECURITY

24. For information classified RESTREINT UE, actual or suspected loss or compromises of security need to be reported only when they present unusual features and/or when it is assessed that actual damage resulted from the loss/compromise.

25. Whenever a loss/compromise of security affecting information classified CONFIDENTIEL UE or CONFIDENTIAL and above received from the other participant is discovered or suspected:

(a) a report giving details of the loss/compromise is to be sent:

(i) by the GSCSO or ECSD to the U.S. Department of State, for US classified information;

(ii) by the U.S. Department of State to the GSCSO or ECSD, as appropriate, for EU classified information

(b) an investigation into the circumstances of the breach/compromise is to be made. When completed, a full report must be submitted to the office to which the initial report was addressed. At the conclusion of the investigation, remedial or corrective action, where appropriate, is to be taken.

SECURITY VISITS

26. The U.S. Department of State, the GSCSO and the ECSD are to facilitate the reciprocal visits referred to in Article 11 of the Agreement to ensure that information released by their parent organisation is properly protected. Such visits are to be conducted as part of a mutually agreed process.

27. The U.S. Department of State, the GSCSO and the ECSD are responsible for the implementation of the standards described in these implementing arrangements. Each participant is to conduct internally the necessary checks to verify that the necessary security measures have been taken in accordance with this arrangement.

LIAISON AND REVIEW

28. The U.S. Department of State, the GSCSO, and the ECSD are to maintain constant liaison to oversee the release and exchange of classified information under the terms of the Agreement. These Offices are to meet to discuss and review matters of common interest and assess the implementation of these standards.

29. Any modifications of this technical security arrangement are subject to the mutual approval by the U.S. Department of State, the GSCSO and the ECSD.