



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 3 June 2003**

**10006/03**

**LIMITE**

**CAB 32  
PESC 274  
COSDP 316**

**NOTE**

---

from : The Secretariat

---

to : Delegations

---

Subject : Security Standards for the Protection of Classified Information exchanged  
between NATO and the EU

---

1. Delegations will find attached the text of the security standards agreed, pursuant to Article 12 of the EU/NATO Security Agreement, between the NATO office of Security, the GSC Security Office and the European Commission Security Office for the protection of classified information exchanged between NATO.
2. On 22 May, the Secretary-General of NATO notified the Secretary-General/High Representative that these standards had been approved by the Security Committees of the respective organisations. On 3 June, the Secretary-General/High Representative responded with a similar notification for the EU side.
3. Accordingly the reciprocal standards set out in the Annex are applicable forthwith.

**SECURITY STANDARDS BETWEEN THE NATO OFFICE OF SECURITY (NOS),  
THE EU COUNCIL GENERAL SECRETARIAT SECURITY OFFICE (GSCSO) AND  
THE EUROPEAN COMMISSION SECURITY OFFICE (ECSO) FOR THE PROTECTION  
OF CLASSIFIED INFORMATION EXCHANGED BETWEEN NATO AND THE EU**

**INTRODUCTION**

1. Pursuant to Article 12 of the NATO-EU Security Agreement, reciprocal standards for the protection of classified information exchanged between NATO and the EU are hereby agreed. NOS, the GSCSO and the ECSO are responsible for the implementation and oversight of these standards.

**PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS**

2. Subject to Article 5(a) of the NATO/EU Security Agreement, positions which require access to NATO or EU classified information (respectively NCI and EUCI) must be identified. Access to EUCI and NCI will be authorised only for individuals who have a "need-to-know". Furthermore, individuals occupying such positions which require access to information classified at or above NATO CONFIDENTIAL or CONFIDENTIEL UE level must have a 'need-to-know' as well as a valid Personal Security Clearance (PSC) issued in accordance with the relevant provisions contained in the respective security rules of NATO, the General Secretariat of the Council and/or the European Commission.
3. The parent National Security Authority (NSA) of the individual concerned is the competent authority responsible for seeing that the necessary security investigations on their nationals/citizens have been carried out in accordance with the respective NATO/EU minimum-security standards.
4. Before being given access to classified information, all individuals who require access to classified information must be briefed on the protective security regulations relevant to the classification of the information they are to access. Those individuals accessing classified information must be made aware that any breach of the security regulations will result in disciplinary action and/or possible further legal action in accordance with their respective security regulations or provisions.

## CLASSIFICATION SYSTEM

5. Classification markings will be used to indicate the sensitivity of the classified information and thus the security procedures and regulations which will apply for its protection. The classifications and their equivalence are as follows:

<b>NATO</b>	<b>EU</b>
NATO RESTRICTED	RESTREINT UE
NATO CONFIDENTIAL	CONFIDENTIEL UE
NATO SECRET	SECRET UE
COSMIC TOP SECRET	EU TOP SECRET/TRES SECRET UE

The NATO or EU marking in the classification line indicates ownership of the information and defines, inter alia, originator rights.

All information originated by one of the Parties and provided to the other(s) shall include an express releasability marking, such as:

NATO SECRET  
RELEASABLE TO THE EU

SECRET UE  
RELEASABLE TO NATO

## REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

6. A registry system is established at NATO, the General Secretariat of the Council and the European Commission for the receipt, dispatch, control and storage of classified information. The EU Council General Secretariat will be the Central Registry for NATO classified information provided to the EU. At each organisation a designated registry will act as the main point of entry and exit for information classified NATO CONFIDENTIAL above or CONFIDENTIEL UE and above, as defined per the respective rules of NATO and the EU. Such registries are established as follows:

(a) for NATO: at NATO HQ and SHAPE (for information to be distributed within Allied Command Europe)

(b) for the EU: at the EU Council General Secretariat

7. Central and sub-Registries will be responsible for:

(a) distribution and control of classified information within their respective organisation(s);

(b) storage of classified information; and

(c) final disposal and/or downgrading and/or declassification of classified information, including the maintenance of destruction certificates for NATO accountable or EU classified information.

8. The NOS, the GSCSO and the ECSO will be responsible for the oversight and control of registries within their respective organisation(s) and will inform their counterparts of the establishment/disestablishment of registries containing each other's classified information.
9. When exchanging classified information, appropriately cleared couriers will be used by both sides and will be granted, upon presentation of the appropriate security clearance certificate, access badges to the building(s) they need to visit to deliver and collect the documents.

#### **ELECTROMAGNETIC TRANSMISSION**

10. The electromagnetic transmission of classified information between NATO and the EU and between the EU and NATO shall be encrypted in accordance with the sender's requirements as outlined in its Security Policies or Regulations.
11. Crypto equipment employed for communications between NATO and the EU must have been certified by the appropriate authority of one of the States designated under Article 5a of the Security Agreement if the level of the information is CONFIDENTIAL or below. When the equipment is intended for the transmission of information classified SECRET and above, it must have been evaluated and approved in accordance with NATO or EU policies or regulations.

#### **BREACHES OR COMPROMISES OF SECURITY**

12. Whenever a breach/compromise of security affecting information classified NATO CONFIDENTIAL/CONFIDENTIEL UE or above is discovered or suspected:
  - a) a report giving details of the breach/compromise must be sent:
    - i) by the GSCSO or ECSO to the NOS, for NCI;
    - ii) by the NOS to the GSCSO or ECSO, as appropriate, for EUCI;
  - b) an investigation into the circumstances of the breach/compromise must 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, must be taken.
13. For information classified NATO RESTRICTED or RESTREINT UE breach/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 breach/compromise in accordance with the respective NATO and EU security regulations.

## **INSPECTIONS/LIAISON**

14. The three Security Offices will facilitate reciprocal inspections to ensure that information originated by their parent organisation is properly protected. In this respect, a joint GSCSO-ECSO team will inspect NATO Headquarters and SHAPE, while the NOS will conduct separate inspections to the General Secretariat of the Council and the European Commission.

## **REVIEW**

15. The three Security Offices will facilitate, as appropriate, the presence of observers on their respective inspections. NOS may observe with respect to inspections of EU Member States relative to the protection of NATO classified information releasable to the EU, and GSCSO-ECSO may observe with respect to inspections of NATO Member States relative to the protection of EU classified information releasable to NATO.

## **LIAISON**

16. The NOS, the GSCSO and the ECSO will maintain constant liaison to oversee the release and exchange of classified information under the terms of the NATO-EU Security Agreement. These Offices will meet to discuss and review matters of common interest and assess the implementation of these standards. Any modifications to this Security Standards document shall be subject to agreement between the NOS, the GSCSO and the ECSO and the approval by the NATO Security Committee and the EU Council Security Committee respectively.