



Council of the European Union  
General Secretariat

**Brussels, 27 May 2016**

**WK 439/2016 INIT**

**LIMITE**

**CSC**

**WORKING PAPER**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

**WORKING DOCUMENT**

---

From:	The Chair of the Council Security Committee
To:	Security Committee
Subject:	Leaks of EUCI and the GSC's response

---

For discussion

**Subject:** Leaks of EUCI and the GSC's response

## **I. Introduction**

1. The Council is occasionally confronted with leaks or unauthorised disclosure of EU classified information. Such compromises may originate in EU institutions or national administrations.
2. At its meeting on 23 September 2014, the Council's Security Committee had discussed this matter on the basis of MD 21/14, highlighting the need for better coordination between the EU and Member States in this regard. It also proposed to establish a chain of communication related to the leakage of information, which would work both ways.
3. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, the relevant NSA or other competent authority is supposed *inter alia* to inform the originator and ensure that the case is investigated.
4. Recent examples of leaks are the unauthorised publication of TTIP documents by Greenpeace (see e.g. [www.ttip-leaks.org](http://www.ttip-leaks.org)) and the open presentation of an EU TTIP non-paper on camera during a news broadcast on a Belgian TV channel. All these documents were classified at the level RESTREINT UE/EU RESTRICTED. The latter one being a Council document, the GSC's Security Office has opened an investigation. Further leaked documents have been published, e.g. on the "Statewatch" website.

## **II. Legal framework**

5. Breaches of security and compromise of EUCI are covered by Article 14 of the Council's Security Rules:

Art. 14(1): "A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this Decision."

Art. 14(2): "Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons."

## LIMITE

6. Where a compromise affects EUCI originating in or held by the Council, an investigation is conducted by the GSC's SO on the basis of Articles 14(4) and 16(2) (d) of the CSR, as well as the SO's mandate laid down in Decision 181/10 of the Secretary-General of the Council on the tasks of the Security Office.

### III. Investigation into a leak or compromise of EUCI

7. The person who detects a compromise or a leak, or who has reasonable grounds to assume that EUCI has been compromised or leaked, informs immediately the SO.
8. The GSC investigation seeks to:
  - identify the compromised document and its originator;
  - identify if possible whether the leak may have originated in the GSC and how the leak occurred.The originator is informed and asked to indicate whether the information is still to be considered as EUCI.
9. The investigation seeks to determine if a compromise of EUCI has occurred, or if there are reasonable grounds to assume that EUCI has been compromised, and whether the leak has originated in the GSC. However, the SO cannot investigate in Member States or other EU institutions.
10. The director of the SO may request the relevant Member States' security authorities and the security services of other EU institutions or international organisations to assist in such investigations.
11. The relevant authorities of the Member States and the GSC shall be notified of the outcome of the investigation and the actions taken.

#### **IV. Damage assessment**

12. A damage assessment is a formal analysis to determine the effect of a compromise of EUCI on the interests or security of the European Union or of one or more of the Member States. It is part of the actions to be taken by the GSC's SO or, where relevant, the respective NSA or other competent authority where it is known or where there are reasonable grounds to assume that EUCI has been compromised.
13. The information available from the incident report, the investigation and the originator shall be the basis to proceed with a damage assessment. A damage assessment report should be prepared and sent to the competent security authority. However, the GSC does not have a developed formal system for conducting damage assessments.

#### **V. Searching for leaks on the internet**

14. The GSC SO would be willing to carry out regular searches for possible EUCI leaks on the internet, and, if compromises of EUCI are encountered, notify the NSA's of the affected Member States. The SO's Investigation Office shall launch an investigation when the compromised EUCI originates in the Council.

#### **VI. Items for discussion in the CSC**

15. The Committee is invited to consider the following questions:
  - Does the Committee agree with the process outlined seeking to involve Member States further?
  - What other steps could be taken?
  - How could coordination between the Member States and between the GSC and the Member States be reinforced?
  - Are Member States carrying out similar searches like those outlined under point 14 or other leakage-related searches, or are they envisaging to do so?

## **LIMITE**

- What factors do Member States take into account when assessing the damage caused by a compromise and how is the damage assessment process organised?
- Should the GSC draw up some common damage assessment guidelines?