



Council of the
European Union

Brussels, 14 September 2017
(OR. en)

12207/17

CSC 205

NOTE

From: General Secretariat of the Council
To: Delegations
Subject: Guidelines on procedures in case of EUCI compromise

Delegations find at Annex the Guidelines on procedures in case of EUCI compromise, as approved by the Council Security Committee on 30 June 2017.

Guidelines on procedures in case of EUCI compromise

I. INTRODUCTION

1. These guidelines, agreed by the Council Security Committee in accordance with Article 6(2) of the Council Security Rules¹ ('CSR'), are designed to support implementation of the CSR, and in particular Articles 14 and 16.
2. They describe the principles and the procedure to be applied where EU classified information ('EUCI') originating in or held by the Council has been compromised, or is suspected to have been compromised.
3. The Council and the General Secretariat of the Council ('GSC') will apply these security guidelines in their structures and communication and information systems ('CIS').
4. When EUCI is handled in national structures and national CIS, the Member States will use these security guidelines as a benchmark.
5. EU agencies and bodies established under Title V, Chapter 2 of the TEU, Europol and Eurojust should use these security guidelines as a reference for implementing security rules in their own structures.

II. PRINCIPLES

6. Breaches of security and compromise of EUCI are covered by Article 14 of the CSR. Article 14(1) reads: "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." Article 14(2) reads: "Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons."

¹ Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information, OJ L 274, 15.10.2013, p. 1.

III. INVESTIGATION INTO A COMPROMISE OF EUCI

7. Any actual or suspected compromise of security must be reported immediately to the competent security authority which will then take the appropriate measures. If an actual or suspected compromise occurs for EUCI held by a Member State, the relevant NSA will inform the GSC's Directorate for Safety and Security ('DSS') and launch an investigation in accordance with the respective national laws and regulations. Where an actual or suspected compromise occurs for EUCI originating in or held by the Council, an investigation is ordered and overseen by the GSC DSS on the basis of Articles 14(4) and 16(2)(d) of the CSR and in accordance with the GSC's internal procedures.
8. An investigation will seek to determine if a compromise of EUCI has occurred, or if there are reasonable grounds to assume that EUCI has been compromised, and to identify:
 - the compromised document, its originator and any other related relevant information (e.g. the status and version of the document, meta data, drafter, etc.); and
 - if possible, where the compromise has occurred, the individual(s) involved and how the compromise occurred.

The originator of the EUCI will be informed and asked to indicate whether the information that has been compromised or suspected of being compromised is still to be considered as classified, and to provide a preliminary assessment of the potential damage that has occurred or will likely occur (e.g. reputational, political, operational, etc.).

9. The Director of the GSC DSS may request the competent security authorities of the relevant Member States and the security services of other EU institutions or international organisations to assist in such investigations if there are indications that the compromise occurred within their jurisdiction.
10. Where a Member State receives such request for assistance, this Member State will examine the information available and determine whether an internal investigation should be launched. The Member State will provide a written reply to the GSC DSS indicating how the request has been followed up.

11. Where a Member State's competent security authority has been informed about an actual or suspected compromise, and has launched an investigation in accordance with paragraph 7, it will inform the GSC DSS and may request the DSS to assist in its investigation.
12. When the GSC DSS receives such request for assistance from a Member State, it will examine the information available and determine whether an internal investigation should be launched. The DSS will provide a written reply to the competent security authority of that Member State indicating how the request has been followed up.
13. The originator of the compromised information will conduct a damage assessment (i.e. a formal analysis to determine the impact of a compromise of EUCI on the interests or security of the European Union or of one or more of the Member States) and forward its findings to the competent security authority undertaking the investigation. Upon completion of an investigation, the competent security authority will draft an investigation report. This report will set out the outcome of the investigation, the actions taken to locate and recover the EUCI, what corrective or disciplinary action has been taken, and what actions have been taken to mitigate the risk of future incidents occurring.
14. The competent security authorities of the Member States and the GSC's Appointing Authority will be notified of the outcome of any investigation and action taken in the light of the incident.
15. The GSC will report any compromise of EUCI to the Council Security Committee at the appropriate time, for example when the investigation has been concluded and where reporting the incident would not hamper or jeopardise an ongoing case. The decision on when to notify the CSC of compromises will be taken by the GSC DSS in a timely manner, in consultation with the originator. Once per year, the DSS will submit to the Committee in a standardised form an overview of compromises of EUCI.
16. Pursuant to Article 14(5) of the CSR, any individual found responsible for compromising EUCI will be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations. Where the individual who has committed the compromise is a GSC staff member, the competent security authority undertaking the investigation will inform the GSC DSS, which will then inform the relevant NSA.