



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 10 January 2005

**16012/1/04
REV 1**

LIMITE

**CSC 23
PESC 1152
JAI 557**

NOTE

From : The Council Secretariat
To : Delegations

Subject : Guidelines on the security clearance of personnel

Delegations will find attached Council guidelines on the security clearance of personnel approved by the Council on 21 December 2004.

These guidelines are designed to cover in particular:

- (a) individuals employed by a civil or military national administration;
- (b) civil servants and other agents employed by the General Secretariat of the Council (GSC);
- (c) individuals employed by a civil or military national administration and who are seconded to a position in the GSC; and
- (d) individuals assigned by a Member State to represent it in Council meetings and in a Council preparatory body where information classified CONFIDENTIEL UE or above is handled.

Council Guidelines on the Security Clearance of Personnel

INTRODUCTION

1. The Council Security Regulations stipulate that the Council and each Member State shall ensure that common minimum standards of security are observed in the Council, all administrative and/or government departments, by EU decentralised agencies and by GSC contractors so that EU classified information (EUCI) can be passed in the confidence that it will be handled with equal care. Such minimum standards include criteria for the clearance of personnel.

2. These guidelines accordingly set out the minimum criteria to be applied for conducting personnel security clearances procedures in accordance with Part I(8) and (9), part II, sections I(2), V and VI of the Annex to the Council decision of 19 March 2001 adopting the Council's Security regulations, for access to EUCI and address the following aspects:
 - (a) personnel security clearances (PSCs);

 - (b) responsibilities;

 - (c) identification of positions requiring an appropriate PSC;

 - (d) criteria for assessing eligibility for a PSC;

 - (e) Investigative requirements for CONFIDENTIEL UE, SECRET UE and TRES SECRET UE/EU TOP SECRET PSCs;

 - (f) requirements for the revalidation of PSCs;

 - (g) procedures for addressing adverse information about an individual holding a PSC;

 - (h) requirements for maintaining records of PSCs granted to individuals;

 - (i) security awareness and briefing of individuals;

- (j) access to EUCI, provisional appointments, one-time access, emergency access, and attendance at conferences and meetings;
 - (k) PSCs for couriers, guards and escorts; and
 - (l) access by non-EU nationals.
3. For the purpose of these guidelines, the following definitions shall apply:
- *Security screening*: investigative procedure conducted in accordance with the relevant rules and regulations in force in the Member State concerned by the competent national authority of that Member State in order to determine the vulnerability of an individual and to provide an assurance that nothing adverse is known which would prevent the individual being granted a personnel security clearance for access to information classified CONFIDENTIEL UE or above;
 - *Personnel security clearance (PSC)*: an administrative decision by the competent national authority of a Member State which is taken following completion of security screening, certifying that an individual may, provided he has a real “need to know”, be allowed access to EUCI up to a specified level;
 - *Authorisation*: an administrative decision by the appointing authority of the Council, authorising access by officials and other servants of the General Secretariat of the Council to information classified CONFIDENTIEL UE and above. Such authorisations may only be issued by the appointing authority following a request for security screening to the competent national authorities of the Member State of which the person subject to authorisation is a national and where such a request has resulted in a positive opinion given by these authorities. For the purpose of these guidelines, an authorisation given by the appointing authority of the Council in accordance with the Council security regulations is to be treated in the same way as a PSC issued by a national competent authority;

- *Personnel security clearance certificate*: a security certificate issued by a competent authority establishing that an individual has been security cleared and showing the level of classified information to which that person may have access, and the date of expiry.

- *Positive opinion*: a notification issued to the appointing authority of the Council by a competent national authority certifying, on the basis of security screening, that an individual may, provided he has a valid "need to know", be allowed access to EUCI up to a specified level. Its period of validity may not exceed the date of validity of the PSC it is based on.

PERSONNEL SECURITY CLEARANCE (PSC)

4. In accordance with the requirements of Council Decision 2001/264/EC, there shall be an agreed standard of confidence regarding the loyalty, trustworthiness and reliability of all individuals granted access to, or whose duties or functions may afford access to, EUCI. In order to achieve this, before having access to information classified CONFIDENTIEL UE or above, individuals shall have a need-to-know, undergo security screening and hold a PSC certificate. These individuals include in particular:
 - (e) individuals employed by a civil or military national administration;

 - (f) civil servants and other agents employed by the General Secretariat of the Council (GSC);

 - (g) individuals employed by a civil or military national administration and who are seconded to a position in the GSC; and

 - (h) individuals assigned by a Member State to represent it in Council meetings and in a Council preparatory body where information classified CONFIDENTIEL UE or above is handled.

**RESPONSIBILITIES OF MEMBER STATE NATIONAL SECURITY AGENCIES (NSAs)
AND THE GSC**

5. NSAs (or other competent national authorities) are responsible for:
 - (a) conducting security screening and issuing personnel security clearance for nationals/citizens who require access to information classified CONFIDENTIEL UE or above, and for conducting screening investigations with a view to providing an opinion to the appointing authority on whether an authorisation should be granted, denied or revoked, as appropriate;
 - (b) ensuring that the common minimum standards of investigation are consistent with those prescribed in paragraphs 9 to 11 below;
 - (c) ensuring that screening investigations are carried out with the knowledge and consent of the individual being investigated in accordance with national laws and regulations, including those concerning appeals; and
 - (d) co-operating with other NSAs or other competent national authorities in carrying out their respective investigations.

6. The GSC and Member States are responsible for:
 - (a) identifying positions which require a PSC;
 - (b) granting access to EUCI within their area of responsibility, including in the situations described in paragraphs 35 to 40 below;
 - (c) ensuring that minimum personnel security standards, as set forth herein, are met; and
 - (d) evaluating continuing eligibility of their staff for access to EUCI.

IDENTIFYING POSITIONS REQUIRING A PERSONNEL SECURITY CLEARANCE

7. The GSC and Member States shall draw up lists of positions which may require access to EUCI. In order to assess whether a particular position requires a PSC, they will involve managers who are most familiar with the work of their staff and the levels of access to EUCI the position may require. It is they who will generally assess the PSC level required for the position.
8. Managers shall also be responsible for ensuring that their staff has the level of PSC certificate appropriate to the access that their work requires and that the need to know principle is strictly applied. When an individual's PSC certificate is due for revalidation, or when the jobholder changes, the appropriate manager shall be responsible for assessing whether the level of PSC remains necessary for that position.

CRITERIA FOR ASSESSING ELIGIBILITY FOR A PERSONNEL SECURITY CLEARANCE

9. The following paragraphs contain the minimum criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for him to be granted and to retain a PSC. These paragraphs consider aspects of behaviour and circumstances that may give rise to potential security concerns.
10. Where appropriate and in accordance with national legislation, a spouse's, cohabitant's or close family member's character, conduct and circumstances may also be relevant and should be taken into account when considering an individual's eligibility for PSC.
11. The minimum criteria for assessing the loyalty, trustworthiness and reliability of an individual for him to be granted and to retain a PSC shall, where appropriate and in accordance with national legislation, include information on whether an individual, his spouse, co-habitant or close family member:

- (a) has committed or attempted to commit, conspired with or aided and abetted another to commit (or attempt to commit) any act of espionage, terrorism, sabotage, treason or sedition;
- (b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such or an associate of representatives of organisations or foreign states, including intelligence services of foreign states, which may threaten the security of the EU or a Member State or States, unless these associations were authorised in the course of official duty;
- (c) is or has been a member of any organisation which by violent, subversive or other unlawful means seeks the overthrow of the government of a Member State or States, or a change in the form of government of a Member State or States;
- (d) is, or has recently been, a supporter of any organisation described in sub-paragraph (c) above, or who is, or who has recently been closely associated with members of such organisations;
- (e) has withheld or misrepresented or falsified information of significance, particularly of a security nature, or has lied in completing the personnel security form in accordance with national laws and regulations or during the course of a security interview;
- (f) has been convicted of a criminal offence;
- (g) has serious financial difficulties or unexplained affluence;
- (h) has a record of alcohol dependence;
- (i) has a record of use of illegal drugs and/or misuse of legal drugs;
- (j) is or has been involved in conduct, including any form of sexual behaviour, which may give rise to the risk of vulnerability to blackmail or pressure;

- (k) has demonstrated dishonesty, disloyalty, unreliability, or untrustworthiness;
- (l) has seriously or repeatedly infringed security regulations, including a failure to protect classified information, or has attempted, or succeeded in, unauthorised activity in respect to communication and information system(s);
- (m) is suffering, or has suffered, from any illness or mental condition which may cause significant defects in judgement or reliability or may make the individual, unintentionally, a potential security risk. In all such cases competent medical advice should be sought; or
- (n) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive or criminal organisations or individuals whose interests may threaten the security interests of the EU and a Member State or States.

DUAL NATIONALITY

- 12. For individuals holding dual-nationality, one of which may be non-EU, special attention should be afforded when considering eligibility for a PSC. Provided that the Member State NSA undertaking the security screening is content that there is no actual or potential conflict of loyalty, there is no *prima facie* reason why a PSC should not be granted.

INVESTIGATIVE REQUIREMENTS FOR CONFIDENTIEL UE, SECRET UE, TRES SECRET UE/EU TOP SECRET PERSONNEL SECURITY CLEARANCES

- 13. The initial issuing of a PSC for access to information classified CONFIDENTIEL UE and SECRET UE shall be based on enquiries covering at least the last 5 years, or from age 18 to the present, whichever is the shorter; and shall include the following:
 - (a) the completion of a national personnel security questionnaire;

- (b) identity check / citizenship / nationality status – the individual’s date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources; for example, due to former residence or past associations; and
 - (c) national and local records check – a check should be made of national security and central criminal records, where these latter exist, and/or other comparable governmental and police records for any officially recorded indication of disloyalty or unreliability. The records of police agencies with legal jurisdiction where the individual has resided or been employed for at least six months should be checked.
14. The initial granting of a PSC for access to information classified TRES SECRET UE/EU TOP SECRET shall be based on enquiries covering at least the last 10 years, or from age 18 to the present, whichever is the shorter. If interviews are conducted as stated in sub-paragraphs (e), (i) and (ii) below, enquiries shall cover at least the last 7 years, or from age 18 to the present, whichever is the shorter. In addition to the requirements stated in paragraph 13 above, the following are required - where provided and admissible under national law and regulations - for clearances for access to information classified TRES SECRET UE/EU TOP SECRET; these factors may also be relevant in security screening for access to information classified CONFIDENTIEL UE and SECRET UE, where appropriate and in accordance with national laws and regulations:
- (a) financial status – information shall be sought on the individual’s finances in order to assess any vulnerability to foreign or domestic pressure due to serious financial difficulties, or to discover any unexplained affluence;
 - (b) education – information shall be sought on attendance since the eighteenth birthday, or during an appropriate period as judged by the investigating security authority, at universities and other education establishments;

- (c) employment – information covering present and former employment shall be sought, reference being made to sources such as employment records, performance or efficiency reports and to employers or supervisors;
 - (d) military service – where applicable, the service of the individual in the armed forces and type of discharge will be verified; and
 - (e) interviews shall be conducted:
 - (i) with the individual, especially if initial enquiries have revealed potentially adverse information; and
 - (ii) also with persons who are in a position to give an unbiased assessment of the individual’s background, activities, loyalty, trustworthiness and reliability. When it is the national practice to ask the subject of the investigation for referrals, referees shall be interviewed unless there are good reasons for not doing so. Sufficient additional enquiries shall be conducted to develop all relevant information available on an individual and to substantiate or disprove adverse information.
15. If any of the requirements or factors outlined above cannot be covered, steps shall be taken to cover these requirements or factors through other investigative means, in accordance with national laws and regulations.
16. The NSA or competent national authority shall consider all available information as part of the security screening procedure. Indications of potential vulnerability to pressure (e.g. debts or the potential vulnerability of a spouse/cohabitant/close family member) need not be a reason to deny clearance if the subject’s loyalty, trustworthiness and reliability are undisputed. The competent national authority shall assess the risks associated with each case in order to determine whether the individual may be granted a PSC.

17. In the event of the appointing authority of the Council either refusing to issue an authorisation to an official for access to EUCI after receiving a positive opinion from the parent NSA, or withdrawing such an authorisation, the parent NSA will be immediately informed in writing by the Council Security Office. Should they consider it necessary, the authorities of the Member State in question may ask the appointing authority of the Council for any further clarification it can provide.

PSC CERTIFICATES

18. With regard to officials and other servants of the GSC, once a NSA or other competent national authority has provided a positive opinion on the granting of an authorisation to an individual, the appointing authority may grant such authorisation and issue a PSC certificate. The annex contains a model of the PSC certificate issued by the Council Security Office.
19. For national officials seconded to the GSC, their national authorities shall provide a copy of a valid PSC certificate to the Council Security Office.
20. Individuals participating in meetings of Council preparatory bodies discussing information classified CONFIDENTIEL UE may only do so following an identity check and confirmation of the individual's PSC certificate. For delegates from Member States the PSC certificate shall be forwarded by the appropriate national authorities to the Council Security Office, or exceptionally be hand carried by the delegate concerned. Where applicable, a consolidated list of names may be used, giving the relevant personal data of the individuals concerned and other details required in a PSC certificate.
21. In all cases, the PSC certificate shall contain the date on which it was issued, the level of classified information to which the individual may have access and its date of validity.
22. If an individual's period of service does not commence within 12 months of the issue of a new authorisation required for a position with the GSC, or if there is a break of 12 months in an individual's service, during which time he or she is not employed in a position with a Member State's civil or military body, the matter shall be referred to the individual's parent NSA for confirmation that the PSC remains valid and appropriate.

REVALIDATION OF A PERSONNEL SECURITY CLEARANCE

23. After the initial granting of a PSC and provided the individual has had unbroken service with a Member State or the GSC and has a continuing need for access to EUCI, the PSC shall be reviewed for revalidation at intervals not exceeding 5 years for a TRES SECRET UE/EU TOP SECRET authorisation/PSC and 10 years for CONFIDENTIEL UE and SECRET UE authorisation/PSC, with effect from the date of the last security screening on which it was based. All investigations for the renewal of a PSC shall cover the period since the previous investigation. Requests for revalidation shall be applied for in a timely manner.

24. For revalidation of a CONFIDENTIEL UE and SECRET UE PSC certificate, the procedures outlined below shall, as a minimum, be carried out:
 - (a) the completion of a national personnel security questionnaire;

 - (b) for officials and servants of the GSC, a check against the security and personnel records of the GSC;

 - (c) after (a) and (b) the completed personnel security questionnaire mentioned at (a) shall be sent to the individual's parent NSA which can request review by the host State, or other Member States in which the individual or, in accordance with national laws and regulations, his spouse, co-habitant or close family member has resided, of its national records.

25. The parent NSA shall then review any information arising during the course of these records checks against the background of its own records and, in the case of officials and other servants of the GSC, forward its opinion to the appointing authority.

26. The revalidation of a TRES SECRET UE/EU TOP SECRET PSC, in addition to the normal review procedures outlined in paragraph 23 above, may include an interview with the individual and shall require the following to cover the 5 years since the last security screening:
- (a) where character references are required by Member States, references shall be taken up in consultation with the NSA of the host State;
 - (b) in the event that a more detailed investigation is required, and where authorised under national legislation, interviews should be conducted with at least two persons who are in a position to give an unbiased assessment of the individual's background, activities, loyalty, trustworthiness and reliability;
 - (c) when a PSC of an individual serving abroad has to be revalidated more than once during uninterrupted expatriation, consideration should be given to undertaking the detailed investigation referred to under (b) above;
 - (d) additional enquiries, where necessary, by the NSA of the host State on behalf of the parent State arising from any information which may come to light as a result of any action under paragraph 24 and 26 (a) to (c) above;
 - (e) the despatch by the NSA of the host Member State and of any other Member State in which the subject has resided, of any information developed within the terms of paragraph 24 and 26 (a) to (d) to the parent NSA of the individual in question;
 - (f) a review by the parent NSA of the individual against the background of its own records;
 - (g) and the despatch of the parent NSA's opinion, with regard to the renewal of the authorisation, to the appointing authority.

27. If, after a revalidation file has been duly introduced with the relevant NSA, a PSC has not been revalidated before its validity has expired, a further period of up to twelve months may be allowed for the revalidation to be completed, provided that the responsible NSA has commenced the action necessary for such revalidation. If, at the end of this additional period, the revalidation has still not been completed, the individual shall be moved to duties that do not require a PSC.

ADVERSE INFORMATION

28. Procedures shall be established to ensure that if adverse information becomes known concerning an individual, a determination shall be made by the individual's parent NSA as to whether he shall continue to hold a PSC. In cases where individuals are considered to represent an unacceptable security risk, the NSA's positive opinion and/or the individual's PSC shall be withdrawn and the individuals shall be excluded from access to EUCI and from positions where they might endanger security. When the PSC is withdrawn for an individual seconded to the GSC, the GSC will be notified by the parent NSA. In the case of officials and servants of the GSC, the parent NSA shall send its opinion to the appointing authority which shall revoke the authorisation in question and shall assign the official to duties not requiring access to EUCI.

RECORDS OF PERSONNEL SECURITY CLEARANCES

29. Records of the PSC granted to individuals for access to EUCI shall be maintained by the Member States and by the GSC as appropriate. These records shall contain details of the level, date and validity of the PSC certificate.

SECURITY AWARENESS AND BRIEFING OF INDIVIDUALS

30. All individuals employed in positions where they have access to information classified RESTREINT UE, or hold a PSC for access to information classified CONFIDENTIEL UE or above, shall be briefed on security procedures and their security obligations. All cleared individuals shall acknowledge that they fully understand their responsibilities and the consequences when EUCI passes into unauthorised hands either by intent or through negligence. A record of such a written acknowledgement concerning access to information classified SECRET UE and above shall be maintained by the Member State and by the GSC, as appropriate.
31. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, contacts with the media, and the threat presented by the activities of intelligence services which target the EU and its Member States. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach they consider suspicious or unusual.
32. All individuals who cease to be employed in duties requiring access to EUCI shall be made aware of, and acknowledge in writing, their responsibilities for the continued safeguarding of EUCI.

GRANTING ACCESS TO EUCI

33. An individual shall only be granted access to information classified CONFIDENTIEL UE or above after he has been granted a PSC, a determination of need-to-know has been made, and he has been briefed on the Council's Security Regulations and has acknowledged his security obligations by signing an appropriate document.

SPECIAL CIRCUMSTANCES

Provisional appointments

34. When an individual is to be assigned in a position that requires a PSC at a level higher than that currently possessed by the individual, the assignment may be made on a provisional basis, provided that:
- (a) the individual possesses a current PSC;
 - (b) action has been initiated to obtain the level of PSC required for the position;
 - (c) no objection has been received from the responsible NSA or other competent authority; and
 - (d) satisfactory checks have been made that the individual has not seriously or repeatedly infringed security regulations.
35. Provisional appointments shall not extend beyond six months from the date the individual takes up the position. The appointment may be extended for another six months if security screening has been initiated and there is no adverse information.

One time access

36. Exceptionally, individuals may be granted access on a one-time basis to EUCI classified one level higher than that to which they are cleared. The following criteria must be fulfilled:
- (a) a compelling mission need for the access shall be justified, in writing, by the individual's supervisor;
 - (b) access shall be limited to specific items of EUCI in support of the mission described by the supervisor;
 - (c) the individual possesses a current PSC;
 - (d) satisfactory checks have been made that the individual has not seriously or repeatedly infringed security regulations;
 - (e) for the GSC such authorisation shall be granted only by the appointing authority or the Head of the Security Office;
 - (f) a record of the exception, including a description of the information to which access was approved, shall be maintained by the relevant registry or sub-registry.

37. This procedure shall not be used on a recurring basis for access to EUCI. If this is required, or if access is required for more than 6 months, a PSC certificate for the higher level must be obtained.

Emergency access

38. In wartime, during periods of mounting international tension, international contingency operations or in peacetime during deployments or on-call/exercise duty when emergency measures require it or when other compelling reasons are present, Member States and the Secretary-General/High Representative or Deputy Secretary-General, may, in exceptional circumstances, grant, in writing, access to EUCI to individuals who do not possess the requisite PSC, provided that such permission is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and reliability of the individual concerned. (A record of this permission describing the information to which the access was given shall be maintained in the appropriate registry or sub-registries.)
39. In the case of information classified TRES SECRET UE/EU TOP SECRET, such emergency access shall be confined wherever possible to those individuals who have been granted access to either national TOP SECRET or to information classified SECRET UE.

COURIERS / GUARDS / ESCORTS

40. Couriers, guards and escorts employed to carry documents classified CONFIDENTIEL UE and above shall, as a minimum and under normal circumstances, possess a PSC for SECRET UE. Couriers, guards and escorts shall be briefed on the Council's Security Regulations and be instructed on their duties for protecting the EUCI they are entrusted with. When individuals are employed in circumstances where they might have accidental access to classified information, they shall be security cleared to SECRET UE or to the level deemed necessary by the relevant security authority.

ACCESS BY NON-EU NATIONALS

41. In accordance with the provisions of the Council's Security Regulations, individuals who are non-EU nationals may be granted access to EUCI classified information on a case-by-case basis, provided that:

- (a) access is necessary in support of a specified EU programme, project, contract, operation, or related task;
- (b) the individual is in possession of a national security clearance based on a clearance procedure no less rigorous than that required for an EU national in accordance with Council's Security Regulations; and
- (c) the prior written consent of the Member State, institution or decentralised agency that originated the information is obtained. Where possible, this consent may grant access to a specific bloc of classified information.

**General Secretariat of the Council of the European Union (GSC)
Personnel Security Clearance (PSC) Certificate**

Certification is hereby given that

Full Name:

Date and Place of Birth:

Position:

Rank/Grade:

Has been issued a personnel security clearance by:

Valid until:

And may, in accordance with the Council decision 2001/264/EC laying down the Council's security regulations, be entrusted with EU classified information up to and including:

- TRES SECRET UE/EU TOP SECRET**
- SECRET UE**
- CONFIDENTIEL UE**

The validity of this certificate will expire not later than:

Date:

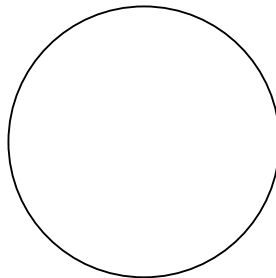
.....

Signed:

.....

Head of Security Office

Stamp:



Date: